Linnæus University
Sweden

Master's Thesis

Internet of Things

Tapping into Security and Privacy issues associated with internet of things

Author: Nabeel Ahmad na222rr@student.lnu.se
Supervisor: David Randall
Examiner: Anita Mirijamdotter
Date: 2021-10-06
Course Code: 21VT-5IK50E, 30 credits
Subject: Information Systems
Level: Graduate
Department of Informatics

Abstract

The Internet of things and its collaborative technologies such as 5G, cloud, artificial intelligence, analytics, and automation will allow people and objects/devices to communicate not only with each other but with any thing at any time and any where using the internet. Nowadays, people interact with different smart devices daily. Keeping in mind technology's evolution, it is estimated that each of us will own roughly 15 linked devices by 2030. Therefore, we cannot neglect the impact of this technology on virtually everything and various risks associated with such emerging technologies.

The goal of this thesis was to better understand the phenomenon of the Internet of Things and more importantly, what security, privacy, and trust threats are associated with it. And how these threats can be overcomed. Moreover, how IoT devices are perceived in terms of privacy and security by people and what factors they must keep in mind while buying, using, and disposing of such devices.

Literature review and interviews were made to better understand the issues of privacy and security in IoT devices and people's understanding of them. A general inductive method proposed by grounded theory was used to analyses the obtained data, and answers were grouped into categories to identify different themes within the data.

The results of the interviews and data showed that people's top priorities with smart home IoT devices were interest in technology, comfort, a better lifestyle, energy savings, and cost savings. People were unaware of the gravity of security and privacy issues by and large, and they had no idea how to counteract them. Common uses of smart devices include virtual assistants, smart heating, listening to music, getting weather and traffic updates, smart lighting, smart lock systems, and fitness gadgets. The results can be seen in the empirical findings and discussion chapters. These results will also be published on relevant Facebook groups and in the local newspaper, Valbyavisen.

Data showed IoT understanding and use of technology was directly proportional to the age factor. Young people were more aware and excited as compared to older ones. Finally, some suggestions were presented on how to buy, use, and discard IoT devices. Future research directions were also presented to conclude the thesis report.

Key Words

Internet, Internet of Things (IoT), Architectures, Components, Security & Privacy, Threats, Awareness, Grounded Theory, Focus Group, Semi Structured Interviews, Technology, Risks, Devices, Qualitative.

Acknowledgements

I would like to thank and express my heartfelt gratitude to all the respondents who spared their valuable time to sit with me, discuss and contribute to my thesis, especially under Covid-19 restrictions and SOPs we had to follow.

My sincere thanks to my supervisor, Prof. David Randall for his very friendly behavior, constant support, and timely guidance throughout the thesis process. He encouraged me to limit the boundaries of my thesis and seek meaningful conclusions. I am truly indebted to his contribution.

I would also like to thank Professor Anita Mirijamdotter for her very thorough and point to point feedback, along with students from the Department of Informatics, as they also provided me with constructive feedback during thesis seminars that set the right course for my work.

Sincerely,

NABEEL AHMAD
Copenhagen, Denmark
28-09-2021

Table of Contents

1. Introduction

2. Literature Review

3. Methodology

List of Acronyms and Abbreviations

AI	Artificial Intelligence
AMQP	Advanced Message Queuing Protocol
CoAP	Constrained Application Protocol
CPS	Cyber Physical Systems
DoS	Denial of Service
DDS	Data Distribution Service
DLRL	Data Local Reconstruction Layer
DCPS	Data Centric Publish Subscribe
FTTx	Fiber to the x
GSM	Global System of Mobile Communication
GTM	Grounded Theory Methodology
GDPR	General Data Protection Regulation
GPS	Global Positioning System
IoT	Internet of Things
IP	Internet Protocol
IDS	Intrusion Detection Systems
IVA	Intelligent Virtual Assistants
IPv6	Internet Protocol Version 6
LAN	Local Area Network
ML	Machine Learning
MQTT	Message Queue Telemetry Transport Protocol
MAN	Metropolitan Area Netwrok
NFC	Near Field Communication
QoS	Quality of Service
RFID	Radio Frequency Identification
UMTS	Universal Mobile Telecommunication
VPN	Virtual Private Network
WSNs	Wireless Sensor Networks
Wi-Fi	Wireless Fidelity
WAN	Wide Area Network

List of Figures

List of Tables

Chapter 1

Introduction

In the introduction chapter, motivation for said research is briefly described, followed by thesis topic and problem background. To establish research questions, practical relevance of research is explained, leveraged by the scientific situation related to the topic. The objective was to relate the scientific work with research topic and expand on it in later chapters.

1.1 Background

The Internet has changed the way we live, communicate, interact, travel, and care about ourselves. A considerable number of the latest home appliances and devices can communicate and interact with each other via the Internet and can be remotely monitored and controlled through applications on our smartphones, e.g. coffee makers, washing machines, light bulbs, vacuum cleaners, alarms, ovens, refrigerators, TVs, music systems, home computers, intelligent virtual assistants, etc. This phenomenon is known as the "Internet of Things," or IoT. Riahi, et al. (2013) said, IoT environments are formed by smart home objects and services interacting autonomously and in real-time.

Governments around the globe like Japan, the UK, and the USA, have invested millions of dollars in the research and development of the Internet of things to promote this initiative (Chan, et al., 2009). It is a technological advancement that has the potential to not only revolutionize ordinary people's lives but also reshape the governments, industries, businesses, and services sectors of the world economy.

The primary goal of consumer IoT is to bring comfort in ordinary people’s lives. For instance, people dislike getting out of their cozy and warm beds just to turn off a light or the television. But now, IoT powered smart home devices can do this for them.

With the help of sensor based technology, people’s home can understand their preferences and can automate themselves to meet them. Such as turning on or off the lights, TV, air conditioner, or fans, or playing music. As objects, devices and appliances become smarter, a smart home can incorporate their capabilities into itself. For instance, laundry schedules can be integrated into smart washing machines. When people are on vacation, their plants can be automatically watered at the appropriate level by sensing the soil's humidity and room’s temperature. When people are about to leave for work or from home, their smart cars can detect this and start or stop itself and can also begin heating or cooling itself.

On the other hand, while IoT benefits individuals, societies and businesses, the next phase of IoT impact will be in the form of smart cities and smart nations. Information and data from homes, neighborhoods, buildings, and institutions are correlated at the city level for better energy management, traffic management, and city planning thus providing additional benefits to ordinary people. Similarly, in the business and industrial world, we can have effective and efficient operation management, automated production and supply lines, optimal use of resources and assets, and improved customer service and experiences.

However, besides these benefits, comes concerns about security risks and breaches of trust and privacy in smart devices. Because in today's world, our devices gather and send data to a variety of 3rd parties, such as home security alarm providers, energy providers, fitness watch vendors, and car manufacturers. Similarly, smart assistants respond to our voice commands and send data over the internet, thus risking possible data breaches. If such information about our presence or absence from home goes into the wrong hands, our security and privacy can be at serious risk. Then, there are concerns about the nature and quantity of the information being gathered by smart devices and ultimately transferred to service providers. Who has access to it, who will use it and how it will be used? is another serious question mark.

If smart devices are not properly managed during their life cycles, each new device can introduce a new security risk. Regardless of whether devices were used by ordinary people, businesses, or governments. All players in the value chain, including the system owners, must manage and mitigate security risks accordingly to safeguard their privacy and security.

Researchers have observed that people don't understand the severity of the situation or think about it the way they should. They are not aware to what extent their personal information is collected by smart devices, thus making the basis of my thesis to answer questions like: how your smart TV is watching you while you are watching television. ...? How can hackers install different spyware in your house using lightbulb security flaws...? and when our central heating system asks for our phone number, which can be forwarded to marketing companies. Therefore, it is the right time to take privacy, security, and safety issues more seriously. People must have a sense of understanding while buying smart devices. They must also consider which factors are crucial while buying and using smart devices.

Lastly, the manufacturing industry is equally responsible for producing secure devices. because hackers and cybercriminals are increasingly targeting connected devices. Therefore, it is the responsibility of manufacturers to produce secure devices, provide appropriate security and privacy checks, and update their devices by providing newer versions, so consumers can fight cyber criminals who are actively attempting to breach their security, infect them with malware, and steal their data.

The next section explains the previous research around the internet of things and its security.

1.2 Previous Research Around the Problem

With the advancements in smart home technologies and the diversification of use cases, interconnected technologies have become an increasingly important part of users' personal lives. The resulting implications have sparked the interest of researchers and practitioners in recent years. In particular, studies focused on privacy and security concerns, people's perceptions, people's understanding and the barriers that prevent the adoption of smart home technologies (Gubbi, et al., 2013).

The Internet of things (IoT) is a buzzword now a day. The concept of connecting physical devices to the digital world is not really a new phenomenon. A lot of research has been done in this area, especially after the rise of the digitalization age in the recent past, where objects are getting smarter and smarter, communicating with each other and transferring data not only to each other but also to other devices and systems is expanding at rapid pace (Riahi, et al., 2013).

According to researchers, the Internet of things (IoT) can be viewed as an extension of IT in different aspects of our daily lives, i.e., the transformation of current networks into new networks in order to establish a globally interconnected heterogeneous network of smart devices (Ramos, Pawlowski, Jara, Gomez and Ladid, 2015).

According to Alaba, Othman, Hashem and Alotaibi (2017), the Internet of Things has created a global network of people, objects, sensors, and services. The primary goal of the Internet of Things is to provide a network infrastructure that enables communication protocols, software, and the incorporation of physical/virtual sensors, personal computers, smart devices, automobiles, and other real-world objects to connect with each other at any time on any network.

The ever-improving capabilities of various network technologies, such as RFID (Radio Frequency Identification), Wireless sensor networks (WSNs), and their increased storage capacity, will result in a plethora of interconnected devices. But people and devices around them require at least one unique identification number that will allow them to communicate with each other (Abomhara and Koien, 2014).

This novel interconnectivity has now turned into an internet of everything, which is a mix of people, processes, data, and things to make network connections more meaningful than ever before. Evans (2012) emphasizes, it is worthwhile to transform information into actions that create new capabilities, increase economic opportunities for individuals, businesses, and nations.

But these new relationships between people and devices have given rise to new kinds of vulnerabilities and threats which were not known, existed or identified before. For instance, integration of different forms of data (structured, unstructured, semi-structured) with emerging technology like IoT has resulted in new security loopholes in personal, organizational and national security systems and vulnerabilities that did not exist in the previous systems (Grossklags and Good, 2007).

Information security is a critical aspect of business for organizations and individuals as a user of information systems. These systems store and share critical information that must be protected against a variety of threats, necessitating the need for a variety of security controls and mechanisms (Mattord and Whitman, 2018).

The Internet of Things is a kind of IS (information system) that must be safeguarded against unauthorized and unauthentic access, disclosures, disruptions, alterations, and modification. According to Vashi et al. (2017), the use of IoT devices as a technology is rapidly increasing, thus creating more and more security and privacy issues. Burg, Chattopadhyay and Lam (2018) stated that the communication in IoT devices happens through wireless infrastructure and networks that connect the devices but simultaneously make them more vulnerable to network threats.

Researcher has observed, the most published material within the IoT domain is related to its structure, protocols, involved technologies, data connectivity, and security/privacy. But I don't think the

published literature is keeping up with people's perceptions of this technology. What opportunities and challenges does this technology pose? Are we ready to deal with them? Are we paying enough attention to them? Do companies give consumer privacy and security the importance they deserve while manufacturing these devices, or are they just reaping profits out of this emerging mass market? That is where I want to dig deeper and form the basis of my thesis report. The next section explains purpose of my research.

1.3 Purpose of the Research

The objective of this thesis was to explore what the Internet of Things is? What are its enabling technologies, components, and architecture? How does it work? Is it really that important? What security, privacy, and trust issues are associated with smart devices?

Furthermore, to provide an insight into people's understanding about the phenomenon, which factors are important for them in terms of security and privacy, and what important points they must consider while buying, using and disposing of these devices. Thesis report also aims to provide the ordinary reader, who has no idea about Internet of Things (IoT) , its systems, its environment and technical terminology, an easy to grasp overview.

The next section describes research questions of the thesis report.

1.4 Research Questions

Based on the discussion in previous sections, my research questions are the following:

I. What security, privacy, and trust issues are associated with IoT devices?

II. How much do people understand and care about security, privacy, and safety in terms of IoT devices?

III. What factors people must consider when buying and using IoT devices?

1.5 Importance and Significance of the Research

This section explained the motivation for my research, which is to further understand the concept of IoT, and to learn about the limitations and weaknesses of this technology in terms of security and privacy with a particular focus on people's understanding of them.

Arguably one of the most important technological development of this century, the Internet of Things (IoT) is going to impact us as individuals, as society, and as businesses around the world equally. But when and how, is not clear at the moment. Currently, we have more than 7 billion connected IoT devices and this number will grow to 75 billion by 2020/21 (Riggins, et al., 2015).

According to technology experts, IoT will take the definition and meaning of inter-connectivity to a whole new level, where devices will start talking to each other. Its influence can be seen now and in the future, from ways to reduce industrial waste, costs, and inefficiency while increasing efficiency and productivity to environmental friendly, cleaner, more productive products and technologies, ultimately leading to a better quality of life.

We can say with confidence that the opportunities and possibilities created by IoT for today and the future are unpresented. For instance, IoT will revolutionize the healthcare and telemedicine industries, from round-the-clock monitoring to 3D printing of human organs and wearable medical technologies. (Greengard, 2015, p.53). Industrial manufacturing will have smart supply chains, while in agriculture, farmers will deploy sensors to manage soil and water treatments.

Greengard (2015) emphasizes the fact that IoT is not just limited to sensing and connecting objects to its surrounding environment but it will be the way to monitor, measure, and understand the perpetual motion of the world and the things people do.

If we gather data from the digital lives of the people, it is predicted that IoT will lead to a global, emerging, ambient, tightly networked computing environment that will rely on smart sensors, cameras, software, databases, and huge data centres with an unimaginable amount of structured and unstructured data (Greengard, 2015 pp.57). Technologists then using augmented reality will be able to convert this data into virtual data and images which can be displayed via wearable and implanted technologies.

Over the years, technology has evolved from monitoring and control of things to Networking of Things, and ultimately to the Internet of Things. This evolution will not stop here but continue to grow. Besides that, we cannot neglect the potential problems and issues created by IoT not only for individuals but at industrial, societal, and government levels.

Riggins, et al. (2015) distinctively pointed out behavioural, organizational, and business-related issues with IoT instead of just focusing on the technology aspect of it. We must not forget the accessibility factor, when talking about IoT and how it can impact different segments of our society.

Noticeable importance has been given to the security, privacy, and trust issues of IoT devices. But considering the future impact of this technology and potential future uses, i.e., the development of smart environments and self-conscious/autonomous devices that have the capabilities to form their own social networks in different dimensions, e.g., smart transport, smart products, smart cities, smart health and smart living, the focal point of research must be on security and privacy factors for now and in the future. As sooner or later, this phenomenon will grow into information security, which contains several layers of security within itself. For instance, from system security to network security, from application security to physical security and software security.

This reason has motivated me to dig deeper into the security domain. Identify the main issues within IoT devices, explain them and focus on what technical mechanisms are involved backstage, critically analyse them and present solutions in the light of academia and industry experts.

Although there have been many studies on security, privacy, and trust issues of smart homes, few have focused on smart home users' privacy acceptance level. It is, however, critical for the successful adoption and rapid spread of smart home technologies (Wilson, et al., 2015).

Figure 1 below depicts the approach taken during establishing the thesis topic and its background.

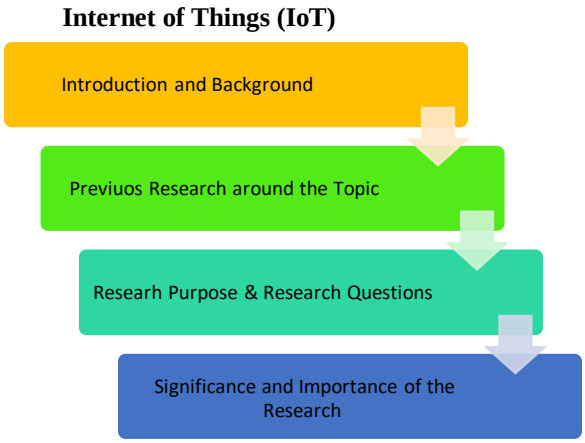
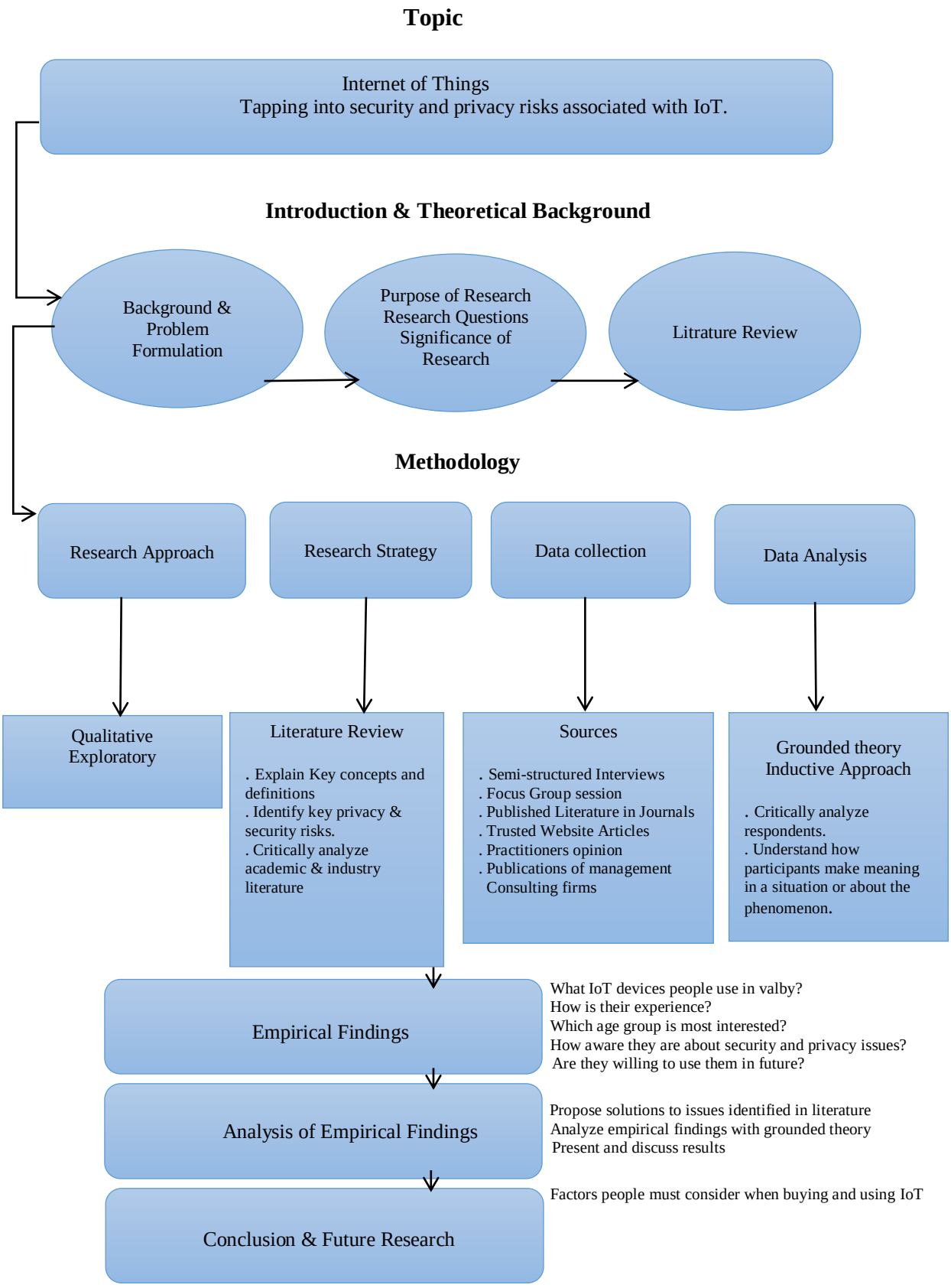


Figure 1: Step by step approach taken in establishing Thesis report topic

1.6 Proposed Model for Thesis



Chapter 2

Literature Review

In the literature review, phenomenon of the Internet of Things is defined and explained along with its architecture, its attributes, its enabling technologies, its operational protocols, its components, and finally how it works. A critical analysis of relevant literature on security, privacy, and trust issues in the context of the IoT' and its impact on people, businesses and industry is presented. The reason was to evaluate the general public's understanding of IoT devices and to educate them, which factors are important when using or buying IoT devices. Explanation of these concepts not only helped to justify the thesis topic but also made it easier for the audience to follow and understand the objectives of the thesis. The literature review is summed up with the identification of key security and privacy issues in IoT devices, both for people and industry.

Literature review findings are immersed with the rest of the thesis to give it continuity, a flow, and a logic with easy-to-understand argumentation.

2.1 Online Search Criteria

According to Creswell (2017) the search criteria for conducting a literature review starts with choosing a topic and evaluating its worthiness, whether it should be researched or not. In the case of my thesis report, it is absolutely clear that internet of things and security" is amongst the most discussed, debated and written topic specially during current technological evolution.

Churchill and Iacobucci (2018) stated academic literature search mainly includes three categories: (a). conceptual literature (b). trade literature (c). Published statistics. How a researcher can use one of these research techniques depends upon the nature of research questions and how theoretical foundations will be laid down. For my thesis, conceptual literature will be collected from renowned and well-established journals in Information Systems, IT, and Business. Trade literature can be gathered from published secondary data of industry professionals and leading management consulting firms. The aim was to conduct literature review in an organized way to capture, evaluate and summarize the literature as suggested by (Creswell, 2017).

On February 1st, 2021, a search was conducted using Linnéuniversitetet's scholarly databases of peer-reviewed literature such as Research Gate, Science Direct, IEEE Explorer, Scopus and Web of Science. Google scholar was also used as a support database to look for relevant articles.

The initial search has been conducted with the term "Internet of Things or IoT", followed by the combination of terms i.e. "Internet of Things" and " Security and Privacy", "Internet of Things" and " IoT components, IoT enabling technologies", "Internet of Things" and " people's awareness", "Internet

of Things" and " important factors", "Internet of Things" and " challenges and opportunities", "Internet of Things" and " Smart Homes ", "Internet of Things" and " Society, Businesses, Industries" and finally "Internet of Things" and " Future Research ".

To improve my literature review process, ensure quality and to give the right reasoning why I chose only relevant articles/research papers and not others, I excluded irrelevant papers and citings.

Table below shows the database search results 570 documents in total, including 250 research papers in IS journals, 100 in IT & Management journals, 150 in Consulting publications, 50 in Industrial publications, 70 in Master theses & books and 50 in Governmental publications. Main subject areas for my online search were Social sciences, IT, Information systems and Management sciences. Later I shortlisted 163 documents of my interest and which were relevant for my literature review.

Table 1: table 1 shows the how online search for literature was conducted

Online Search Process		**Documents**
Search Words Internet of Things, IoT Risks, Security and privacy Industrial IoT, Smart homes Architecture, Components Challenges, Opportunities People, awareness, knowledge Protocols, Enabling technologies Steps, Measures, Suggestions Future Research and IoT	List of Databases Science Direct IEEE Explorer Research Gate Scopus Google Scholar Web of Sciences	
Search Result Total		570
Search Language	English	
Source Type	IS journals, 250 IT & Management journals, 100 Consulting publications, 150 Industrial publications, 50 Master theses & books, 70 Governemntal publications, 50	570
Document Type	Empirical scholarly work i.e. research articles, research reports, conference papers, case studies, dissertations, textbooks. Dissertations, newspaper editorial/opinion pieces .	
Which subject areas were searched	Social sciences, IT , Information systems. Management sciences.	

Following keywords were used to search for right information from diversified sources.

Table 2: table 2 shows keywords used to search databases

No	Key Words
1	Internet of Things, IoT
2	Risks, Security and privacy
3	Industrial IoT
4	Smart Homes
5	Architecture, Components
6	Challenges, Opportunities
7	People, awareness, knowledge
8	Protocols, Enabling technologies
9	Steps, Measures, Suggestions
10	Future Research and IoT

Articles published in selected leading and widely accepted academic MIS journals are used to capture the relevant data. List is mentioned below:

Table 3 : table 3 shows list of the databases used to look for the relevant information

No	List
1	Science Direct
2	IEEE Explorer
3	Research Gate
4	Scopus
5	Google Scholar
6	Web of Sciences

2.2 What is Internet of Things (IoT)

In 1999, Kevin Ashton of Procter & Gamble tabled the term "Internet of Things for the very first time. In simple words, the Internet of Things (IoT) is a network of objects that are embedded with sensors, software, and other related technologies mainly for connecting, exchanging, and transferring data with other devices and systems via the internet. These devices may range from simple household objects to complex business and industrial tools and technologies.
We can say that it is an ecosystem where humans, objects/devices, and the internet interact with each other, intersect with each other and gives birth to IoT as seen in figure 1 below.

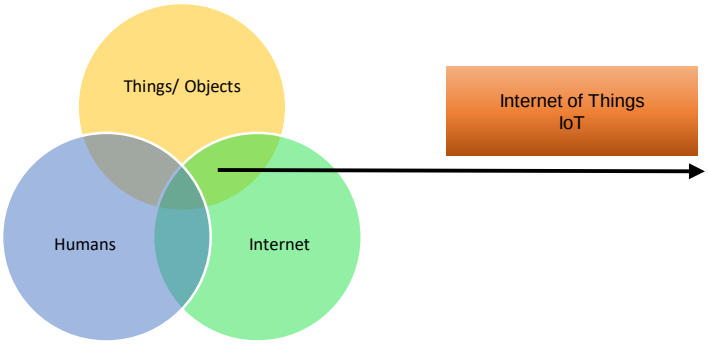


Figure 2: simple illustration of IoT adopted from (Stojkoska and Trivodaliev, 2017)

According to Stojkoska and Trivodaliev (2017), Smart objects that are capable of communication and computation with each other are present everywhere around us. For instance, ranging from simple sensors, home appliances, sophisticated smartphones to industrial devices. These heterogeneous networks of such objects/devices come under the umbrella of a phenomenon known as the Internet of Things. Vermesan and Friess (2013) explain the Internet of Things (IoT) is a network that allows heterogeneous objects to connect at any time and any place over the internet.

During the past 5-6 years, the Internet of Things (IoT) has received considerable attention from academic researchers and the business world. It is now considered one of the most vital elements of Industry 4.0 (Perera, et al., 2014).

There were more than 50 billion IoT devices until 2020 and it is expected that these devices will generate 4.4 zettabytes of data in 2021. Financial returns or revenue generated in the IoT market is similarly astonishing, it has been forecasted that the IoT market will range from $1.6 trillion to $14.4 trillion in 2025, influencing nearly every sector of the economy and human life e.g. transportation, medical care, agriculture, homes, vehicles, schools, markets and industries (Al-Fuqaha, et al., 2015).

Thanks to the Internet of Things (IoT), billions of devices, objects, and gadgets are now connected via the internet around the globe. Collecting and sharing data and exchanging valuable information. Gubbi, et al. (2013) endorsed this capability of IoT by stating, it is an interconnection of sensing and actuating devices, enabling their capability to share information across platforms through a unified framework and developing a common operating picture for enabling innovative applications.

The Internet of Thing's (IoT) vision is to transform the Internet by creating networks of billions of wirelessly recognizable objects / devices that can communicate not only with each other at anytime and anywhere, but with anything and everyone. One method of achieving this is by increasing RFID processing capacities, more wireless sensor networks (WSNs), and storage capacity at lower costs, which will result in the development of a highly decentralized common pool of resources linked by a dynamic system of networks (Borgohain, et al., 2015).

In reality, communications in the IoT can occur not only between devices but also between people and their surroundings. In IoT systems, people, cars, computers, books, TVs, cell phones, clothing, food, medicine, passports, luggage, and other everyday items require a unique identifier allowing them to communicate with one another (Soullie, 2014).

The Internet of Things will have a significant positive impact on citizens, businesses, and government. Ranging from assisting governments in reducing healthcare costs and improving quality of life to reducing carbon footprints, increasing access to education in remote underserved communities, and improving transportation.

2.3 What are Internet of Things (IoT) Devices

According to Radoglou Grammatikis, Sarigiannidis, and Moscholios (2019), the Internet of Things is made up of many networks in which devices can communicate with one another via the Internet. These devices are commonly referred as a 'things' and are depicted in figure 3 below. Each of these 'things' has its own set of attributes.

Figure 3: Attributes of IoT devices adopted from (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019)

2.3.1 Identification

This is the first attribute of IoT devices. Each IoT device must be uniquely identifiable within the network. To assign unique addresses to network objects, two methods, IPV4 and IPV6 are used. Initially, IPV4 was used for addressing, but as the number of objects has grown, IPV6 is being used now for its 128 bit addressing scheme (Burhan, Rehman, Khan, and Kim, 2018).

2.3.2 Sensing

Sensing refers to gathering data from the physical environment (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019). Various sensing devices such as smart sensors, actuators, and RFID tags are used to collect data from devices (Burhan, Rehman, Khan, and Kim, 2018).

2.3.3 Communication

This process involves sending and receiving data, messages, files etc., via connected devices. Technologies like Bluetooth, wireless networks, RFID, and others are used to communicate between objects.

2.3.4 Computation

Computation is used to process the data obtained from the IoT devices (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019). This process is also used to eliminate extra or un-necessary data. Various hardware and software platforms are available to perform computation on collected data (Burhan, Rehman, Khan and Kim, 2018).

2.3.5 Services

Services refer to those functions of the devices that are provided to users based on the information they receive (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019).

2.3.6 Semantics

It is the final attribute of IoT devices. It refers to the ability of IoT devices to obtain correct information from their physical environment and provide that information as a service at an appropriate time or when required (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019).

2.4 How Internet of Things (IoT) works

Internet has changed the world and how we work & communicate with each other, and this will continue to evolve with the induction of technologies like 5G and new internet protocols like Li-Fi.

Internet of things (IoT) has taken this connectivity to a whole new level by connecting multiple devices simultaneously through the internet, thus not only facilitating man to machine but also machine to machine interactions (Stojkoska and Trivodaliev,2017). This capability opened doors to unimaginable opportunities to exploit for both personal and business levels.

The functioning and application of Internet of things (IoT) is not as complicated as it sounds, but it largely depends on how tech-savvy is the audience. Youngsters and young families are expected to utilize it more than old-age people (Vermesan and Friess, 2013).

In a simple IoT system, devices with built-in sensors are connected to an IoT platforms that collect, exchange, and integrate data from the different devices and then apply smart analytics to exchange vital information with associated applications built to cater to specific needs (Suciu et al., 2013).

These capable and powerful IoT platforms have the ability to point out, what information is required and can be useful and what can be ignored. Collected information can be used for various purposes from detecting patterns, make recommendations, detecting possible problems to smart decision making (Al-Fuqaha et al., 2015).

For instance, if I own a sports clothing and accessories business and I am interested in knowing which optional sports accessories (fishing tools, skating accessories, skiing accessories) are most popular among customers. This can be achieved by applying an Internet of Things solution. I can use sensors to see and detect which areas in the shop are the most popular and where customers spend the most time. Based on this information I can re-align my business strategy, to check which items are selling fast and to make sure hot selling items don't run out of stock while saving time and money at the same time.

IoT Ecosystems are not limited to a particular sector of the economy. IoT business applications are versatile and influence nearly all fields e.g. home automation, vehicle automation, production automation, medical, retail, healthcare, defense, financial sector, and many more (Alcaide et al., 2013).

IoT systems can also use artificial intelligence (AI) and machine learning to make data collection easier and more dynamic.

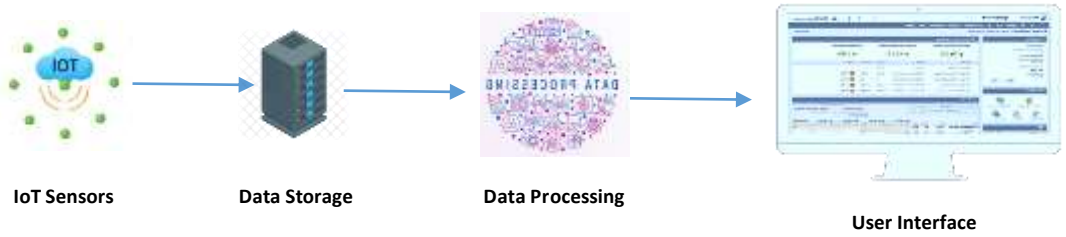


Figure 4: How internet of things works adopted from (Stojkoska and Trivodaliev,2017)

2.5 Components of Internet of Things (IoT) Eco System

IoT Ecosystems are based on different components and their integration such as: artificial intelligence (AI), sensors/devices, internet/connectivity, data processing/analytics and a user interface. I will explain them one by one:

2.5.1 Devices

IoT devices are different types of hardware like sensors, gadgets, home appliances, and machines, that are programmed for certain applications and can transmit data over the internet. These hardware components can be embedded into other mobile devices, industrial equipment, environmental sensors, medical devices, defense equipment, and many more (Miorandi, Sicari, De Pellegrini, and Chlamtac, 2012). That's why, these devices can be used in anything from lights, fridges, security alarms, locks, printers, webcams, home and industrial meters, speakers, cellphones, washing machines, ovens, vacuum cleaners, headphones to wearables gadgets. These devices range from simple to sophisticated structures and can collect and share data, thanks to the availability of affordable computer chips and the presence of high-speed wireless networks.

2.5.2 Sensors

Sensors are another vital component of IoT systems. These devices can detect and monitor external environments, then replace that information with a signal that humans and machines can read and distinguish (Abdmeziem and Tandjaoui, 2014). Sensors can be active or passive and analogue or digital. The most commonly used sensors in IoT systems are the following: Temperature Sensors, Humidity Sensors, Pressure Sensors, Proximity Sensors, Level Sensors, Accelerometers, Gyroscopes, Gas Sensors, Infrared Sensors, and Optical Sensors. They play a critical role in improving operational efficiency, reducing costs, and enhancing workers safety and effectiveness (Curt and Srivastava, 2001).

2.5.3 Connectivity

Connectivity via the internet is the main highlight of IoT devices. These connecting networks are scalable depending upon the IoT system's size and scope (Hu, Peng Tay and Yonggang Wen, 2012).

They range from LAN (Local Area Network): which is a group of devices that are linked together in a single physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network in an office or school with thousands of users and devices (www.cisco.com).

PAN (Personal Area Network): which is a personal area network concerned with the exchange of information in close proximity to a person. These systems are typically wireless and involve data transmission between devices such as smartphones, personal computers, tablet computers, and so on. The purpose of such a network is usually to allow data or information transmission between devices or to server. The IEEE 802.15 working group is in charge of most developments in the field of Personal Area Networks (Finlay, 2016).

MAN (Metropolitan Area Network): which is a computer network that connects computers within a metropolitan area. That can be a single large city, a group of cities and towns, or any given large area with multiple buildings. A MAN is larger than a LAN but smaller than a wide area network (WAN).

MANs are not required to be located in urban areas; the term "metropolitan" refers to the size of the network, not the demographics of the area served (www.cisco.com).

To WAN (Wide Area Network): which is a collection of interconnected local-area networks (LANs) or other networks. A wide area network (WAN) is essentially a network of networks, with the Internet serving as the world's largest WAN. There are several types of WANs available today, each designed for a specific use case that touches almost every aspect of modern life (www.cisco.com).

2.5.4 Artificial Intelligence (AI)

Individually, within their onw right, the Internet of Things (IoT) and Artificial Intelligence (AI) are very productive and powerful technologies but when combined, they become even more effective. when a system can complete a list of tasks or can read and learn from data in an intelligent way is normally termed as artificial intelligence (Burhan, Rehman, Khan and Kim, 2018). When artificial intelligence is mixed with the IoT technology and result is a device, that can analyse data and make intelligent decisions without human involvement is the essence of IoT concept. Figure 5 shows the main components of a simple IoT system.

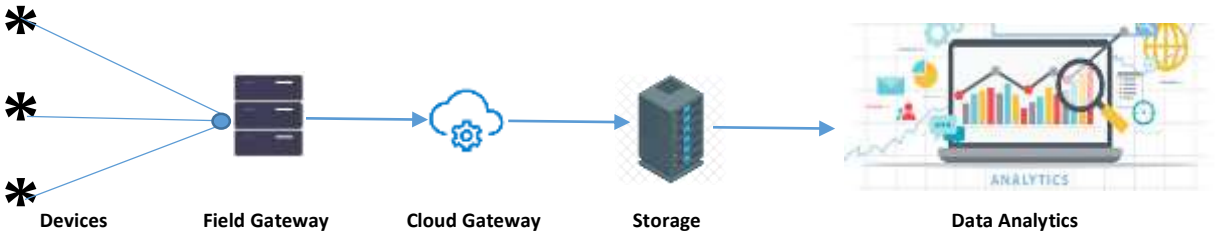


Figure 5: A basic structure of a IoT system adopted from (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019)

2.6 Internet of Things (IoT) and its Enabling Technologies

There are number of technologies that facilitate and enable the internet of things for its smooth functioning namely: Internet protocol 6 (IPv6), radio frequency identification (RFID), wireless sensor network (WSN), intelligent sensing devices, near field communication (NFC), cloud computing (CC), global positioning systems (GPS), service-oriented architectures (SOA), geographic information systems (GIS) and cellular devices (3G/4G/5G). Among these mentioned technologies, three are considered the core technologies for optimal working of the internet of things i.e. IPv6, RFID, and WSN. Figure 6, below highlights various technologies used in an IoT system of different scales and sizes (www.cisco.com).

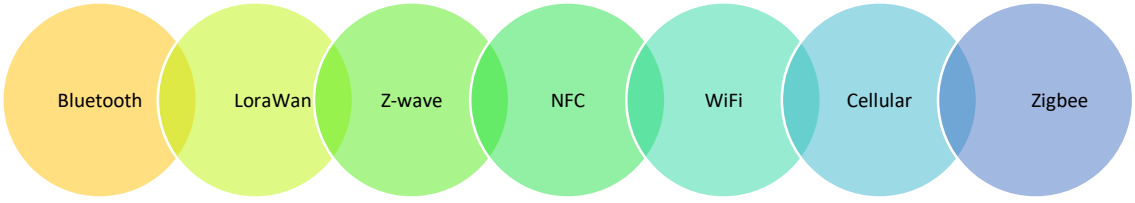


Figure 6: Main technologies & protocols behind IoT Systems (https://data-flair.training/blogs/)

Now I will briefly explain these three core enabling technologies of a IoT system.

2.6.1 Internet Protocol version 6 (IPv6)

The internet protocol version 6 (IPv6) is the most advanced and cutting edge protocol for the Internet's network layer. IPv6 is designed by developers to address various issues of the current version of the internet protocol suite (IPv4) e.g. depletion, safety/security, auto-configuration, extensibility, and scalability. IPv6 has expanded the abilities of the Internet to enable new kinds of technologies such as the Internet of things.

2.6.2 Radio Frequency Identification (RFID)

Radio frequency identification is one of the main enabling technologies of the Internet of Things. Although, its use in the commercial and private sectors is quite new. RFID uses electromagnetic fields to automatically identify and track tags attached to objects/devices. It consists of two components: RFID tags and RFID readers (Glover and Bhatt, 2006).

RFID tag is a device that is attached to the object we want to track or wish to collect data for. and an RFID reader is a device that can feel/recognize the presence of an RFID tag and is able to read the data stored on it (Glover and Bhatt, 2006). RFID technology retrieves data from tagged objects wirelessly with the use of radio waves (Whitmore, Agarwal, and Da Xu, 2014).

RFID tags are of three types: passive, semi-active, and active tags. Passive RFID tags are devices that don't have their own power supply. They obtain their power by modifying the electromagnetic radio wave that the RFID reader sends when querying it for data (Glover and Bhatt, 2006). A semi-active tag has a small power supply but gets power from other sources to complement its limited power supply (Glover and Bhatt, 2006).

Whereas, active RFID tags have their own built-in power supply to power their microchip and sensors (Glover and Bhatt, 2006). IoT devices usually operate for extended periods of time, therefore Passive RFID devices are more suitable for the internet of things because they fulfil their power consumption requirements from other sources.

2.6.3 Wireless Sensor Networks (WSN)

Wireless sensor networks (WSN) are sensor devices geographically distributed in a predefined indoor or outdoor environments and settings. They are used for monitoring and recording the physical conditions of the environment and organizing the collected data at a central point (sinks), where it is being forwarded to a data repository for processing (Benabdessalem, Hamdi, and Kim, 2014). These central points (sinks) for data collections are very powerful as they handle all incoming data, process it, and then send it back to the back-end system.

2.7 Protocols for Internet of Things (IoT)

Since the Internet is the key enabler for IoT systems to function. So a TCP/IP protocol stack similar to the one used for the Internet is also suitable for IoT systems. Therefore, in this section, I will outline some of the standard protocols defined for IoT ecosystems. There are also a number of communication protocols used in the internet of Things (IoT). Some of the main IoT Communication Protocols are Bluetooth, Wi-Fi, Radio Protocols, LTE-A, and Wi-Fi-Direct. These protocols are used in various capacities to fulfil the specific functional requirement of an IoT system and its working. Following are the main protocols used in IoT devices.

2.7.1 Constrained Application Protocol (CoAP)

This is an internet utility protocol designed for devices with limited resources. It was created to allow simple and limited resource devices to connect to IoT systems over constrained networks with limited bandwidth. This protocol is used for machine-to-machine (M2M) communication and was created specifically for Internet of Things (IoT) systems that use HTTP protocols. Constrained application protocol uses UDP protocol for normal implementation. It also uses restful architecture which is similar to HTTP protocol. It uses DTLS for the problem-free switch of statistics within the slipping layer (Glover and Bhatt, 2006).

2.7.2 Message Queue Telemetry Transport Protocol (MQTT)

Message Queue Telemetry Transport is a messaging protocol co-developed by Andy Stanford-Clark of IBM and Arlen Nipper of Arcom in 1999. It was created primarily for M2M (machine to machine) communication and remote tracking in IoT environments. Its primary purpose is to collect data from different devices, objects, and gadgets. This protocol links devices and networks to software packages and middleware. MQTT protocols assist TCP in facilitating secure and dependable information sources (Glover and Bhatt, 2006).

There are three main components of this protocol namely: subscriber, publisher, and dealer. The writer generates the data and transmits the data to the subscribers via the dealer. Then the dealer guarantees security by move-checking the authorization of publishers and subscribers.

2.7.3 Advanced Message Queuing Protocol (AMQP)

JP Morgan's John O'Hara came up with this protocol. The Advanced Message Queuing Protocol (AMQP) is a message-oriented middleware infrastructure software layer protocol. It uses message transport warranty primitives to ensure a smooth and secure verbal exchange. These Internet of Things protocols are made up of hard and fast components that route and save messages within a broker carrier, as well as a collection of policies for connecting the components (Glover and Bhatt, 2006). They make it possible for patron services to interact with dealers and the AMQP model. the three components of this protocol are as follows:

- Exchange: which receives messages from publishers and routes them to message queues.
- Message Queue: Which stores messages until they are thoroughly processed through client software.
- Binding: Which describes the connection between the message queue and the change.

2.7.4 Data Distribution Service (DDS)

Through the submit subscribe technique, data distribution service provides a scalable, real-time, accurate, better overall efficiency, and interoperable statistics shift. Multicasting is used to deliver high-quality QoS to IoT applications. DDS is available on a variety of platforms, ranging from low-footprint devices to the cloud, and it supports green bandwidth consumption as well as agile framework component orchestration.
DDS – IoT protocol has following layers: facts centric submit-subscribe (DCPS) and statistics-local reconstruction layer (DLRL).

- DCPS layer performs the task of handing over the facts to subscribers.
- DLRL layer provides an interface to DCPS functionalities, allowing sharing of distributed data amongst IoT enabled devices.

These above mentioned protocols are the most important ones to understand the technical side of IoT environment.

2.8 Architecture of Internet of Things (IoT)

Over the years, various researchers have presented different versions of IoT architectures, that are equally accepted by Academia and industry. IoT technology is made up of several technologies that work together. IoT devices are made up of sensors, actuators, processors, and transceivers. Sensors and actuators are devices that interact with their physical surroundings. Then in order to derive meaningful outcome from the data collected by the sensors, it must be intelligently stored and processed (Sethi and Sarangi, 2017). IoT devices are normally geographically separated and communication between them happens through wireless mediums. And these mediums are always facing risks like unreliability, distortion and cyber-attacks.

2.8.1 Three Layer and Five Layer Models of IoT

A well-defined IoT architecture is yet to emerge. But a three-layerd high level architecture is generally accepted. This fundamental architecture was presented in the early days of IoT evolution (Wu, Lu, Ling, Sun, and Du, 2010). These three layers are namely: perception, network, and application layers.

2.8.1.1 Perception / Sensing Layer

The perception layer's main task is to perceive the physical properties of things around us that are part of the IoT ecosystem. This perception process is based on a variety of sensing technologies such as RFID, WSN, GPS, NFC, etc. This layer is also in charge of converting information into digital signals, which are more suitable for network transmission. However, some objects may not be sensed directly. Therefore, microchips are needed to be attached to these objects to provide sensing and even processing capabilities (Sethi and Sarangi, 2017).

Nanotechnologies and embedded intelligence can play critical roles in the perception layer. The first role can be to a create chips that are small enough to be implanted into everyday objects and second role can be to enable them with the processing power required by any future applications.

2.8.1.2 Network Layer

The network layer is in charge of processing the data received from the Perception Layer. It is also responsible for transmitting data to the application layer via different network technologies such as wireless/wired networks and local area networks (LAN). FTTx (Fiber to the x), 3G/4G, Wi-Fi, Bluetooth, ZigBee, UMB and infrared technology (Sethi and Sarangi, 2017). Network layer transports massive amounts of data, therefore it is critical to provide reliable middleware for storing and processing this massive amount of data. Cloud computing is the right option in this layer for data storage and processing.

2.8.1.3 Application Layer

Network layer's processed data is used by the application layer. This layer serves as the front end interface of the overall IoT architecture, allowing IoT potential to be realized. This layer also provides the necessary tools (e.g., actuating devices) for developers to realize and materialize the IoT vision (Wu, Lu, Ling, Sun, and Du, 2010). The possible applications are very diversified (e.g., intelligent transportation, logistics management, identity authentication, location-based services, safety etc.). In figure 7 below application layer, network layer and sensing layer of a simple three IoT architecture can be seen.

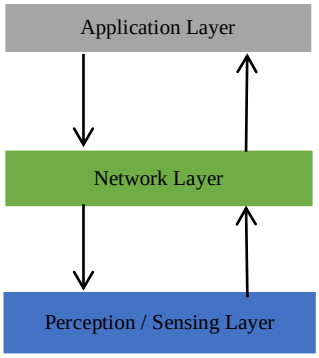


Figure 7: A three-layer IoT architecture adopted from (Wu, Lu, Ling, Sun, and Du, 2010)

Over the years, with technological advancements and significant improvements in IoT systems themselves, more layers were added in IoT architecture model namely: processing and business layers thus turning it into a five-layer architecture model (Mashal, Alsaryrah, Chung, Yang, Kuo and Agrawal, 2015). The five layers' model is the most comprehensive explanation of IoT architecture as shown in the figure 8 below. In this model, the role of the perception and application layers is the same as in the three layered model. Now I describe how the remaining three layers work.

2.8.1.4 Transport layer

The transport layer routes sensor data from the perception layer to the processing layer (middleware layer) via networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.

2.8.1.5 Processing layer

Processing layer is also known as middleware layer. It receives, stores, analyzes, and processes massive amounts of data from the transport / Network layer. It is capable of managing and providing a wide range of services to the lower layers. It makes use of a variety of technologies, including databases, cloud computing, and big data processing modules.

2.8.1.6 Business layer

This layer is responsible for controlling the entire IoT system, including all applications, business models and user privacy and security. The success of any device is determined by not only the technologies used in it but also how these technologies are delivered to their users. These tasks are handled by the device's business layer. It facilitates creation of flowcharts, graphs, analyzes results, and determines how the device can be improved (Sethi and sarang, 2017). Figure 8 below shows inter connectivity between five-layer model of Inter of Things.

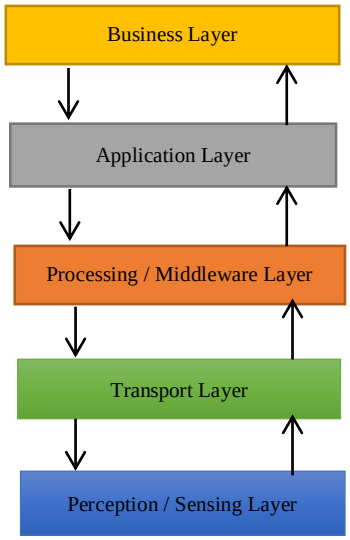


Figure 8: A Five-layer architecture models of IoT adopted from (Mashal, Alsaryrah, Chung, Yang, Kuo and Agrawal, 2015)

2.8.2 Security & Privacy Threats in Different Layers of IoT Architecture

The Internet of Things is a layered architecture, with each layer having its own set of functionalities and employing different technologies to carry out those functions. The rapid proliferation of IoT devices raised different type of security concerns. This section discusses potential security threats in different IoT layers. For instance, authentication, authorization, confidentiality, integrity, privacy, self-configuration, software authenticity, hardware anti-tampering, availability, key management and Trust are potential threats (Cerullo et al., 2018). These threats hide themselves within different layers of IoT architecture and needed to be addressed accordingly.

2.8.2.1 Perception Layer Threats

The perception layer's primary function is information gathering. For this purpose, perception layer employs sensors e.g. RFIDs, barcodes etc. But due to its wireless nature, the criminals can attack its sensor nodes (Vashi et al., 2017). This layer is divided into two sections: Perception nodes (sensors, controllers) and the perception/ sensing networks that connect to the network layer (Alaba, Othman, Hashem and Alotaibi, 2017).

Some examples of perception / sensing layer threats are: Node capture Attacks, Malicious code Injection attack, False data injection attack, Tampering, Eavesdropping and interface attacks and Jamming.

2.8.2.2 Network Layer Threats

Network layer is also known as the transportation layer. This layer relays on the information gathered by the perception layer (Vashi et al., 2017). Network layer is responsible for network transmission, information security and spreading information in the perception layer. Mobile devices, cloud and internet networks are examples of network layer (Alaba, Othman, Hashem and Alotaibi, 2017). This layer facilitates interaction between the application and the service (Li, et al., 2016).

Some examples of Network layer threats are: Phishing site attack, Access Attack/Man-in-the-Middle attack, DoS attack, DDos attack, Sybil attack, Routing attacks/sinkhole attack and Hello Flood attack.

2.8.2.3 Middleware Layer Threats

Middleware layer serves as an interface between the network and application layers. This layer also offers advanced computing and storage capabilities. The middleware layer has features such as device discovery and management, big data analytics, security etc. While the middleware layer provides a dependable and robust IoT interface, it is also vulnerable to a variety of attacks (Hassija, et al., 2019). Furthermore, this layer can retrieve, process, and compute information, and then automatically make decisions based on the computational results. The middleware layer has two critical functions: service management and storing lower layer information in a database (Vashi et al., 2017).

Some examples of Network layer threats are: Flooding attack in cloud, De-synchronization, SQL injection attack and Man-in-the-Middle attack.

2.8.2.4 Application Layer Threats

The application layer is the outermost layer and is exposed to the end user. The foundations of this layer are various applications such as smart grid, smart city, smart government, smart healthcare, and smart transportation (Alaba, Othman, Hashem, and Alotaibi, 2017). This layer has its own particular security and privacy issues which are not present in other layers of IoT architecture.

Some examples of Application layer threats are: Data theft attacks, Data corruption, sniffing attacks, DOS attacks, Malicious code injection attacks and Reprogram attacks.

2.9 IoT and its Impact on People, Society, Businesses & Industries

There are four interconnected components of the IoT ecosystem (people, objects, software, and hardware) that communicate over public and private networks. These networks can be secured and unsecured. The untrusted and unsecured networks give rise to the issues of security, privacy, and trust (Borgohain, et al. 2015).

Personal data is shared or is shareable without the consumer's knowledge in the current age of smart devices. This is due to the fact that data collection has now become passive – performed behind the scenes by the sensors and other data-collection mechanisms built into these smart devices. This trend indicates that consumer information collection has shifted from being actively provided by the consumer to being passively accessed without the consumer's knowledge (Gubbi, et al., 2013).

Analytics commoditization is an emerging concept fed by big data, analytics, and smart algorithms created by social media, consumer goods, FMCG, home appliances companies to gather consumer data. Personal data required for purchasing products and services has become economically viable; personal data can now be traded or monetized. Data commoditization driven by analytics and artificial intelligence has changed the meaning and value of consumer data, thus raising privacy concerns for consumers (www.gartner.com).

Over the years, several security and privacy concerns have risen as a result of the rapid growth in the usage of IoT devices and applications. When virtually everything is connected to everything else, this problem will only get worse and continuous exposure will simply expose more security bugs and vulnerabilities. Hackers can now take advantage of such limitations in IoT technology. Exposed vulnerabilities and weaknesses in an environment of billions of devices is an open invitation for exploitation. There is a risk that loopholes and malfunctions in the IoT systems can overshadow all of its potential benefits if sufficient protection is not put in place (Gubbi, et al., 2013).

Consumer data is normally stored in outsourced third party cloud storage locations by organizations. These vendors can easily get hold of the majority of consumer sensitive data. As a result, cloud service providers now have unrestricted access to consumers' data without the need for any privacy contract. Organizations are the primary customers of cloud service providers not the consumers. The greater the distance between the data keepers (cloud services provider) and the real owner of the data (consumer), the more likely unethical behavior will occur and the risks of data breach will increase (Priya, Pathak and Tripathi, 2018).

Organizations and their supply chain partners can now collaborate within and across the supply chains thanks to B2B integration. Personal data accumulated by various organizations has now been integrated into these cross-organizational supply chains, resulting in a unified digital profile of billions of consumers and giving rise to privacy concerns (Mattord and Whitman, 2018).

For instance, technology giants like Google, Facebook, Microsoft, EBay, and Amazon have compromised user trust on so many occasions by tracking or sharing data they were not authorized to, either on purpose or through system hacks. But still, they are a vital part of our daily and digital lives. The amount of data modern-day smart devices collect is enormous, but what exactly these gadgets and devices are collecting varies from device to device and is based on terms of service agreements, and local regulatory frameworks.

Let's take the example of intelligent virtual assistants (IVA) like Google Assistant, Cortana, Alexa, and Siri. They know about us more than we know about ourselves, e.g. our location, what we buy, where, and when we buy groceries, clothes, and other things of our interest, our travel plans, our health status, our taste in music and movies, and our likes and dislikes. They know when we are at home or coming home, what our voice sounds like as compared to family members and friends. and whether we've paired them with other smart devices in home or not, and what some of those devices are sensing or can sense. Apparently, this data is used to make one's smart device experience better, personalized, and joyful, but what if all this information goes into the wrong hands.?

Borgohain, et al. (2015) explained security issues affecting the IoT technology and integration of such technologies. He particularly highlighted distributed denial of service (DDoS) attacks. In Oct 2016, a large section of the internet was shut down temporarily and so many websites and social media applications were un-accessible, e.g. Twitter, the Guardian, Netflix, CNN, and Reddit. The sole reason was the largest DDoS attack ever faced by the internet community, particularly inflicted on the service provider Dyn through an Internet of Things botnet. This IoT botnet was created via malware named Mirai. This malware-infected computers and Internet of Things devices by penetrating into their passwords without the owner's authorization (Ahmad, 2018). Such attacks are increasing alarmingly, e.g. by 30% from 2017 to 2018 with an increase in average attack size of 543% because of the lack of authentication, authorization, privacy, safety and security of IoT devices (Abrams, 2018).

The majority of devices ask for personal information from users, e.g. name, age, gender, email address, home address, current location, phone number, and access to social media profiles, when we want to connect with them. This information can be very handy for hackers (Fowler, 2017). Devices that are not secured are always at risk of being attacked. These attacks can be like the above-explained Mirai malware or personal identity or personal information theft (Ahmad, 2018).

Lots of IoT devices come with embedded cameras, microphones, and speakers in them. Parents who purchase baby monitors with Wi-Fi connectivity may face a security threat since these baby monitors can be easily hacked from virtually anywhere in the world (Flannigan, 2016). In 2017, Germany's Federal Network Agency declared the smart doll named "My Friend Cayla" an illegal espionage apparatus. Officials state the doll has a hidden microphone that can record and collect the personal conversations of children without any consent for collection, use, or disclosure of this data (Joseph, 2019).

People who have installed different IoT devices such as smart lock systems and indoor fire alarms connected with Bluetooth and/or Wi-Fi may not be as safe as they think, because University of Michigan researchers hacked into these devices without much effort (www.post-gazette.com). They managed to successfully open electronic locks, changed preset device settings of different objects, and remotely triggered a false fire alarm. Smart TVs also track nearly everything people do with their remotes. This information is then sold to third parties for monetary purposes.

The rapid speed of innovation has resulted in requirements for millions of devices, the majority of which are network (mainly wireless) connected in some way. Unfortunately, at the software and infrastructure levels, most of these devices have little to no protection. (Medaglia and Serbanati, 2010).

Security has been characterized by researchers as a structured framework consisting of concepts, values, principles, policies, procedures, techniques, and measures necessary to protect individual system assets and the system as a whole from any intentional or unintentional attacks. Both of these

interactions must be protected, to ensure the data and service provisioning to all parties and to limit the number of incidents that can affect the IoT ecosystem (Miller and Rowe, 2012).

Yoon, et al. (2015) and Suo, et al. (2012) also identified security threats faced by IoT devices and suggested focusing on self-configuration and self-security with minimal human intervention. Granjal, et al. (2015) examined the current IoT protocols for each layer (business, application, transport, network and sensing) of the IoT device's architecture to ensure secure communication.

Keoh, et al. (2014) elaborated on IoT standards such as 6LoWPAN and CoAP defined by the IoT governing bodies. He suggested different measures to secure IoT protocols like DTLS (Datagram Transport Layer Security) and IPSec (Internet Protocol Security). He also explained in detail the usability factor of these protocols.

Khoo (2011) explained security issues concerned with RFID (Radio Frequency Identification) technology in IoT protocols. Sicari et al. (2015) argued that a lot of attention has been given to authenticity and confidentiality factors when it comes to the security and privacy of IoT devices, but researchers have failed to explain these issues and threats faced by other protocols collectively. Instead, they focus in their research papers on individual and specific risks associated with IoT protocols.

For instance, Erguler (2013) examines and evaluates the protocol defined by Zhu, et al. (2012) and says that the authentication factor is very vulnerable when it comes to cyber-attacks, besides it was the main highlight of the research paper of Zhu, et al. (2012).

Shi, et al. (2014) also evaluated the security overview developed by Luo, et al. (2014) for IoT devices. His model uses certificate less online/offline sign encryption, a term introduced by Shi. it is a method that allows encryption and signing of the information under one umbrella and allows for authentication, confidentiality, non-repudiation, and integrity. His study found that an attacker was able to obtain the private key of the sender by performing operations on intercepted messages.

Ndibanje, et al. (2014) pointed out that the protocol developed by Liu, et al. (2012) is too costly to implement simply because of redundant messages being sent out thus increasing the overhead of the respective IoT device. Moreover, the protocol designed by Liu, et al. (2012) proved to be vulnerable to authentication attacks and this design deficiency was improved by Ndibanje, et al. (2014) later.

Kasper, et al. (2014) evaluated actual devices that were sold to people and came up with facts that some manufacturers were using proprietary algorithms and low-cost mechanisms, which ultimately led to compromises in trust, confidentiality, and authentication. Furthermore, Patton et al. (2014) indicated that some of the technology available to the general public is extremely vulnerable, especially from small-scale and lesser-known manufacturers. In some cases, default and very weak passwords were used by manufacturers for their IoT device connectivity.

Skarmeta and Moreno (2014) explained the privacy, trust, and security issues associated with the deployment of IoT devices. They provided a good overview of security analysis of constrained devices by highlighting security architectures based on dynamic trust models. They concluded that more scalable (up & down) and secure protocols needed to be developed for IoT devices of the future. They emphasized that cryptography like new standards and algorithms (hash functions, elliptic curve cryptography, and pairing-based cryptography) should be developed to make IoT devices more secure.

Moving on to IoT and its impact on businesses, McKinsey's Global Institute quoted that the Internet of Things will have an economic effect of $4 trillion to $11 trillion by 2025 (www.mckinsey.com). Companies will gain value by generating new revenue sources such as connected solutions and services for customers and businesses besides lowering their operational costs. The Internet of Things (IoT) will be one of the driving forces behind the Industry 4.0 revolution, as it allows improved automation, data collection, analytics, workflows and process optimization.

Organizations that have lost revenue as a result of the worldwide COVID-19 lockdowns are searching for new ways to innovate and save costs. And digital application of the Internet of Things (IoT) is proving to be one of the main cost-effective and innovative option going forward. But it is not an easy or smooth way forward (www.mckinsey.com).

If we look at the world's top management consulting firms' analysis on the business sector's IoT adoption, they share similar views, i.e., it's difficult to implement IoT technologies and achieve organizational goals with them. Current organizations have little to no experience in implementing these solutions. Integrating emerging technologies like IoT requires well-defined strategic plans, the right resources, timely execution, as well as monitoring and evaluation afterwards. Technology executives must have a thorough understanding of the corporate goals and the CEO's strategic vision for successful implementation of such technologies. And to make sure, the results are in line with the strategic plans, they need to work closely with the organization's relevant stakeholders.

Since modern workplaces are becoming increasingly dependent on mobile devices; organizations are encouraging workers to bring their own devices to work. Although organizations have some control over the hardware and software that workers can use on their personal devices, they have little control over on their overall security (Garba, Armarego, Murray, and Kenworthy, 2015). As a result, the possibility of data leakage and accessing an organization's sensitive information on devices with low-level security tools has increased many folds recently.

Gartner's 2018 IoT Backbone Survey said, security is the top barrier for the IoT success of 32% of IT leaders (www.gartner.com). And in the coming years, figuring out how to reconcile the benefits of IoT-connected devices with possible security risks will be a key element to discuss.

As the Internet of Things becomes more and more common, the CIO in a company needs to step up and lead the charge for success with this technology. Recent studies show, in almost all industries, it is considered to be the job of the CIO to drive the IoT initiative in companies. Therefore, modern-day CIOs are now called "CIO of everything," who can adapt to the company's vision, decision-making, and skills radically to drive the IoT environment. To design and develop the enterprise's IoT involvement, the CIO of Everything will need a dedicated IoT team. This team must be capable of planning, mapping, reading, developing, and managing the company's internal and external IoT domains and products (Cook and Das, 2007).

A curious, entrepreneurial, and strategic-thinking IoT-focused team will help the company's CIO in predicting opportunities and challenges of IoT technology as the dynamics of business, market and technologies change rapidly.

Organizations will view these IoT systems from a variety of perspectives. That's why the ability to act with pace, creativity, and courage are the traits expected from the CIO of everything, regardless of the point of entry for a company into the IoT world. They will be required to own, adapt to, and address

the waves of new and unexpected requests, considerations, and issues IoT technology is going to generate on a daily basis (Hypponen and Nyman, 2017).

Hypponen and Nyman (2017) said the Internet of Things devices do have technological issues, which makes them vulnerable to attacks. They indicated that there is a serious issue with the IoT system's software update. The Internet of Things device's operating system and applications must both be updatable, which is difficult to do at present. Some IoT devices come with pre-installed and obsolete operating systems, which makes them vulnerable even before being used. IoT is no longer just a technological initiative. Organizations that are applying IoT solutions are constantly focusing on the technology's business outcomes. IoT programs are no longer solely motivated by the desire to boost internal operations. Legacy approaches bind IT and business partners in their efforts to align IoT programs with business goals in order to improve sales and the consumer experience. Organizations with a high degree of IoT maturity have a higher rate of success with IoT adoption and are better prepared to survive security threats.

The Internet of Things (IoT) is becoming increasingly popular. Simultaneously, the environment for IoT enabling technologies is also changing and evolving. The maturation of the Internet of Things not only provides opportunities but also some serious worries for organizations. Industry 4.0 and the Internet of Things (IoT) promise creative business models and novel user experiences with the help of strong networking capabilities and efficient use of next generation embedded devices. But at the same time, large quantities of security-critical and sensitive data is also generated, processed, and exchanged, thus making itself a lucrative target for criminals and cyber thieves. (Byres and Lowe, 2004) and (Koscher, Czeskis, Roesner, Patel, Kohno and Checkoway, 2010) and (Miller and Rowe, 2012).

Emerging trends like analytics, automation, artificial intelligence, cloud computing and big data are becoming critical drivers of industrial innovation and production systems. Now, complex supply chains are monitored and optimized using cloud-based services. Machine failures can be predicted using big data algorithms, which decreases system downtime and maintenance costs. With the help of interconnected production systems, processes can be tightly integrated and optimized, and production steps can be outsourced to other sites and businesses for profit maximization. Cloud-based services will soon be forced to consider consumer preferences in product development and planning, allowing for a new level of product individualization at a low cost (Kagermann, Wahlster, and Helbig, 2013). All these developments are breeding grounds for continuously creating security threats.

Moving on to industrial IoT, the "pervasive digital presence" landscape compels managers to rethink digital security by introducing four key differences from conventional IT security: size, diversity, feature, and flow. Security and risk managers in IoT device manufacturing companies must think about how these differentiators are causing change and then devise new tactics to deal with the ever-changing environment (Sadeghi, Wachsmann and Waidner, 2015).

Previously connected devices, particularly in industrial manufacturing, automation and control systems must be able to safely and securely communicate with new connected devices. There is no single protocol for device-to-device authentication or how devices can safely connect to cloud services, due to the sheer variety of devices and different environments in which they operate (Hernandez, Arias, Buentello and Jin, 2014).

It is critical to ensure the integrity of industrial IoT devices, especially their data, against malicious modifications in order to ensure the proper and secure operation of IoT systems in industries (Zonouz, Rrushi, and McLaughlin, 2014). Many security loopholes in embedded systems have been found in

recent studies. This adds to the difficulty of designing and implementing secure embedded systems, which usually must have multiple functions such as security and real-time guarantees at a low cost (Costin, Zaddach, Francillon and Balzarotti, 2014) and (Cui and Stolfo, 2010) and (Soullie, 2014).

It is estimated that by 2022, the Internet of Things (IoT) will be involved in more than 30% of identified attacks in the industry, despite accounting for only less than 10% of IT security budgets. (Gartner research, 2021). Modern industries use cyber-physical production systems (CPPS), which are relatively easy to integrate with the current information security systems of industrial units.

Cyber-physical systems (CPS) are freely programmable embedded devices that control physical processes and are steadily replacing programmable logic controllers. Cyber-physical systems (CPS) usually communicate over closed industrial networks, but they are often linked to the Internet as well (Sadeghi, Wachsmann and Waidner, 2015). There are several positive distinctions between traditional IT systems and CPPS (Kumar and Patel, 2014), thus making it more suitable for modern industrial units.

The number of computing components in industrial control systems, production systems, and factories are steadily increasing. Due to the increasing number of inter-connected CPPS (Cyber-physical systems) and the ability to analyse data collected by CPPS (Cyber-physical systems) using big data analytics, privacy has become a critical consideration.

To address these security and privacy risks, industrial IoT systems require a comprehensive cybersecurity definition that addresses the various security and privacy risks at all levels. E.g. Platform protection, safe engineering, security management, identity management, and industrial rights management are all facets of this. During the life span of smart IoT systems and devices produced, protection and privacy must be maintained throughout the process. In the sections that follow, I will look at ways to secure embedded devices, which are at the heart of cyber-physical production systems (Shahrjerdi, Rajendran, Garg, Koushanfar and Karri, 2014).

People on the industrial side of IoT need to know and understand the threats in their production and supply chain setups, create a strategy, address the security and privacy issues, implement security solutions and in the end equip their employees with the skills necessary for running the IoT-led production facilities. (Kagermann, Wahlster and Helbig, 2013).

Based on findings from the literature review, privacy, data security, authentication, confidentiality, and data integrity are the key issues, among others, when it comes to securing IoT devices, but threats like cryptographic mechanisms, network protocols, data & identity management, and trusted architectures also needed to be addressed. Researchers and industry professionals agree on the below mentioned security and privacy issues as the biggest threats while using IoT devices both in the consumer and industrial sectors.

Authentication, authorization, confidentiality, integrity, privacy, self-configuration, software authentication, hardware anti-tampering, availability, key management, and trust.

These issues will be discussed in detail in the next section. Figure 9 below shows security & privacy issues arising from different layers of an IoT system architecture presented by Mendez, Papapanagiotou and Yang (2017).

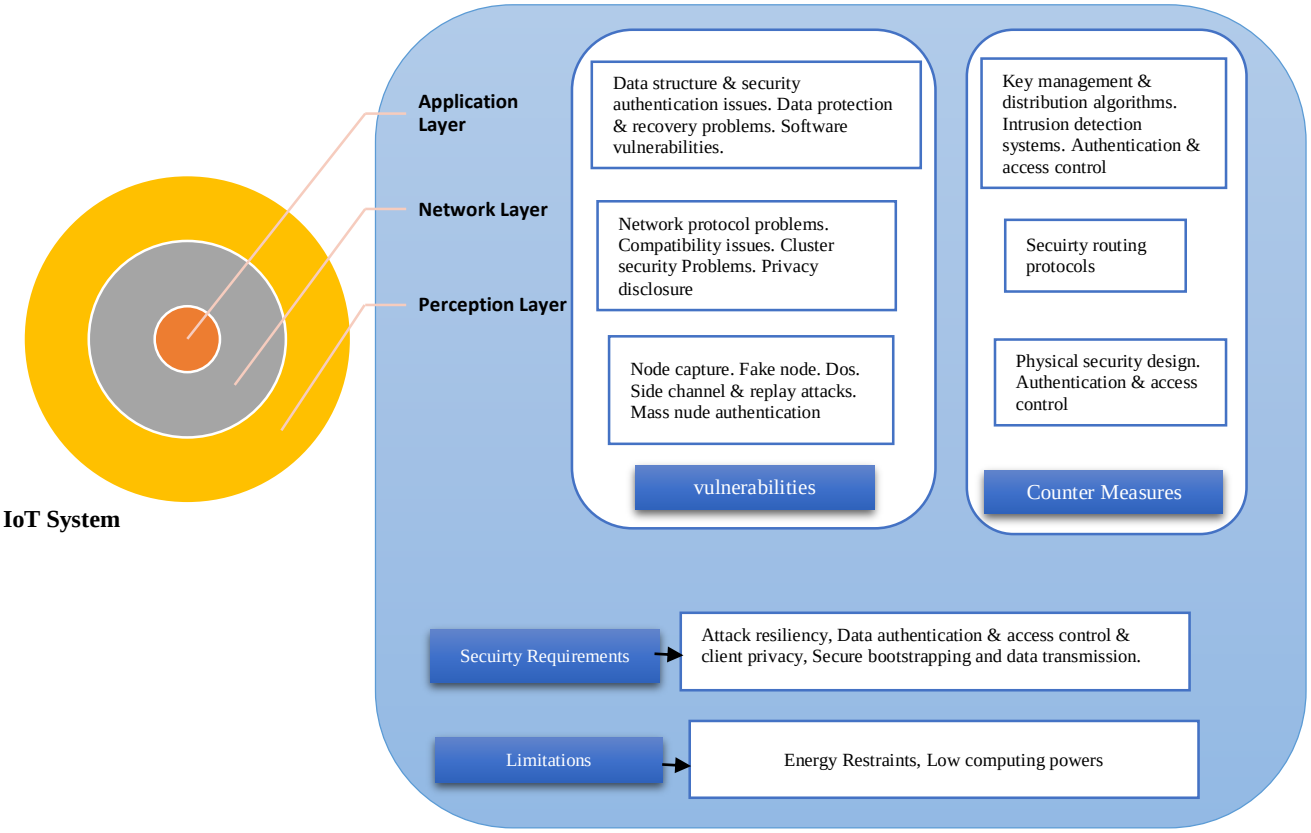


Figure 9: Internet of Things Security Landscape adopted from (Mendez, Papapanagiotou and Yang, 2017)

2.9.1 Authentication

In the dictionary of identity and access management (IAM), authentication validates that users are who they claim they are. and not spyware, viruses, or malicious users pretending to be someone they are not. We, being humans, do this all the time in our daily lives where we differentiate people on the basis of their facial features, hair color, voice, and physical appearance.

This authentication and identification process must not be limited to users and electronic devices, but we also need to know with whom they are communicating. In IoT devices/gadgets, authentication becomes even more crucial, since the majority of communications is done without any user interaction. The capability to ensure that the correct people have access to concerned devices, sensors, and systems for data extraction is an important security concern (Sicari, Cappiello, Pellegrini, Miorandi, and Porisini, 2014). It is also vital to make sure that the data, commands, and requests are sent by the correct and verified devices.

The majority of current embedded systems deploy device authentication methods that rely primarily on a software-based approach, i.e. Trusted Platform Module (TPM), the main example of HRoT implementation, when this collaborates with software-based PKI, creates and delivers high-level trust

authentication for IoT objects. The objective here is, to safeguard data and control access when data travels through an unsecured network such as the internet.

Every IoT device requires a unique digital identity while connecting to a gateway or a central server to prevent malicious actors from sinking in and gaining control of the system. This can be done by attaching an identity to a cryptographic key, unique for every IoT device. And these keys can be issued by the trusted platform module (TPM) and globally trusted Certificate Authority (CA).

2.9.2 Authorization

Another important security challenge in IoT devices is authorization and access control. Authentication deals with device identification, whereas authorization gives permissions. And after looking at current IoT security approaches, we can clearly differentiate between home and industrial IoT environments with very different security threats. In both cases, importance should be given to situations where a single device is communicating with several other devices or back-end computers/servers (Seitz, Selander and Gehrmann, 2013).

This factor also prevails. Even if the particular device is primarily configured by one person in a household or organization, it must be able to handle connections from other devices, and these different devices may not have the same access rights. This means a specific IoT device must be able to distinguish between requests from other devices and execute smart authorization decisions accordingly (Seitz, Selander and Gehrmann, 2013). Furthermore, due to the scalability ability of IoT environments, it is not difficult to predict that some devices can be compromised. That's why authorization checks ensure a restriction on hackers' operations, especially in case of a system breach.

IoT devices use both authentication and authorization, to do role-based access control and make sure that devices only have access and permission to do exactly what they are required to do. And only authorized devices can interact and communicate with other devices, applications, cloud platforms, and network gateways. Figure 18 explains one way, two ways, and three ways of authorization and authentication systems used in IoT devices.

2.9.3 Privacy

Generally, privacy is narrated as the right of individuals to decide when, how, and to what extent their personal information can be revealed and communicated to others. Besides the technological benefits and economic potential of IoT, it is widely accepted that privacy has become one of the major concerns within IoT environments, which seriously hampers the further development and deployment of IoT infrastructures, platforms, services, and applications (Wang, et al., 2015).

It's also worth noting how traditional security mechanisms like identity access management, intrusion detection and response systems, data encryption, and security management may face entirely new design requirements and challenges in IoT-driven use cases (Wang et al., 2015).We must concentrate on how to achieve end-to-end privacy by ensuring the authenticity, integrity, and confidentiality of information collected from various IoT devices, secure network transmission, integration, and aggregation at middleware and edge computing devices, and privacy data analytics at IoT infrastructure (Wang et al., 2015).

To achieve this target, applications of existing cryptosystems and security protocols may not be sufficient and efficient enough. It is rather imperative to develop a set of cryptographic primitives and

protocols, which should be data-driven and with IoT awareness. Privacy can be further subdivided into two factors, i.e., anonymity and digital forgetting, which also play a vital role in ensuring privacy. I will describe them now one by one.

2.9.3.1 Anonymity

Data anonymity refers to removing personally identifiable information from data stored or transmitted through devices so that the people whom the data is about to remain anonymous and secret. Given the huge quantity of data that IoT devices generate and are expected to generate, and with big data exploration, anonymity becomes even more important.

2.9.3.2 Digital Forgetting

Digital forgetting refers to removing pieces of data or data traces from the digital world. Soon there will be IoT devices in their billions, generating a humongous amount of data, both necessary and unnecessary. Therefore, it is important to remove or erase data that is of no use or not required anymore (Xu, Wendt and Potkonjak, 2014).

2.9.4 Confidentiality

Confidentiality means that, apart from the authorized persons and entities involved in a system, the exchanged data during communication is kept confidential. And normally, this is achieved through encryption. Ensuring the confidentiality of data is very crucial in IoT devices because they unobtrusively and ubiquitously collect data, which may be very sensitive and valuable in nature, and normally people do not want to disclose their personal information. Confidentiality can be secured by implementing encryption and cryptographic mechanisms, and this is particularly important when two IoT devices transmit and exchange information with each other (Ashraf and Habaebi, 2015).

2.9.5 Integrity

Data integrity means accuracy and consistency of data stored in a database or a data warehouse, which can be on-site or remotely located (cloud). Some researchers insist on the physical integrity of data, which refers to the process of storing and collecting data in the right way and maintaining its accuracy, validity, and reliability. Whereas, the logical integrity of data emphasizes whether data is correct and accurate in a specific context, like IoT ecosystems in my thesis case. Data integrity also ensures the quality of data in different systems (Sicari, Cappiello, Pellegrini, Miorandi, and Porisini, 2014).

Data integrity is of utmost importance for IoT devices as the accurate collection of data by sensors is required for the IoT devices to function properly and deliver expected results. Systems must ensure that malicious attacks and data modification are not possible if any breach occurs. Integrity can also be achieved by applying collision-resistant hash functions and digital signatures (Ashraf and Habaebi, 2015).

2.9.6 Self Configuration

Since the Internet of Things (IoT) is supposed to connect billions of devices to the Internet, It would be impractical to ask users to manually communicate with and configure these devices in order for them to work. As a result, it's critical that these devices be able to self-configure and dynamically

handle access control systems without user intervention, or at the very least with minimal user intervention (Skarmeta, Ramos and Moreno, 2014).
For instance: Kim recently acquired eight new Internet of Things (IoT) devices, which he plans to incorporate into his home network. It would most likely be inconvenient for him to manually set up each of these new machines.

The Internet of Things, on the other hand, is built to connect anything. As technology advances, it is anticipated that even supermarkets will be linked to the Internet of Things in the near future. As a result, due to the increase in the number of devices, it will become more difficult for him to manually configure and maintain them. It's worth mentioning, that this problem isn't all about safe boot-strapping; it also concerns how devices function and configure themselves during regular usage. Adaptive security, as studied by Hamdi and Abie (2014), is one potential way to do this, as it enables nodes to adapt to the environment as well as their own state while implementing security mechanisms.

2.9.7 Availability

When it comes to IT systems, availability ensures that the system should be up and running for legitimate users at all times. As a consequence, system uptime should be maximized to allow for proper system operation. Owing to the limited existence of IoT devices, which makes them vulnerable to energy-draining attacks, maintaining availability for IoT environments is much more difficult than for conventional Internet environments.
The denial of service (DoS) and distributed DoS (DDoS) attacks, in which an attacker floods the network with unwanted traffic in order to block access to legitimate users, are typical attacks against availability. This type of attack is popular on the Internet, and the Internet of Things has inherited this flaw. Since certain IoT devices help in saving lives, availability is a critical factor. A good example of this is in the field of health care, where the processing of real-time data is important for terminally ill patients.

2.9.8 Trust Management

Since, IoT networks rely on sensor devices to collect data, establishing the trustworthiness of a system and ensuring that it sends back accurate and valid data is crucial. As a result, without implementing trust mechanisms, it would be impossible to determine whether or not the system is working properly.

Furthermore, general cryptographic control mechanisms only secure the validity and authenticity of data and devices. As a consequence, devices that are unreliable or have been compromised and provide incorrect data can go unnoticed. Given this context, the authentication, confidentiality, and integrity of the information being transmitted are perfectly fine from the network's perspective since it is all coming from a legitimate device. However, the precision or consistency of the data can be a concern. This is the reason why trust management is critical since it helps us to track when a system acts oddly or abnormally (Jing, Vasilakos, Wan and Qiu, 2014). One potential solution for maintaining trust in IoT environments is intruder detection systems (Raza, Wallgren and Voigt, 2013).

2.9.9 Key Management

It is mainly concerned with the management of security keys, which is quite crucial considering the size of IoT systems. Especially because, if the security keys are made available to an attacker or if the attacker obtains them in any other way, the attacker would be able to retrieve data sent from IoT

devices. Moreover, key management encompasses key generation or development, key delivery, key change or modification, and key destruction or revocation, in addition to securely storing security keys (Jing, Vasilakos, Wan and Qiu, 2014). This is normally accomplished by generating keys, using secure key exchange protocols, and storing them, using encryption mechanisms.

2.9.10 Software Authenticity

The IT framework must ensure the authenticity and credibility of software installed on devices and systems. This is particularly true in IoT environments, where compromised software may allow security mechanisms to be bypassed. For instance, if malware on an IoT system copies and forwards all of the data it gathers to an attacker's computer, bypassing all security measures can be catastrophic. On the Internet today, making sure, software vendors sign their software is a popular way of defending against this threat.

2.9.11 Physical Security of Devices

IoT devices and systems are likely to run unattended in unprotected environments, such as city streets, parks, public buildings, and parking lots. As a result, attackers can easily gain access to them, increasing the likelihood of physical attacks as well as the probability of tampering (Roman, Najera and Lopez, 2011). This highlights the importance of integrating anti-tampering mechanisms into embedded chips in IoT devices to help deter attacks such as reverse engineering and system tampering. Integrating hardware elements and using hardware values as part of the key generation process are two possible anti-tampering strategies. The physical un-clonable functions (PUFs) are an example of this. They are used to ensure that if an intruder tampers with the device, the device's properties will be changed, forcing the keys to change (Cherkaoui, Bossuet, Seitz, Selander and Borgaonkar, 2014).

Lastly, there are plenty of novel security threats and challenges for devices, networks, operating systems, communication tools, and even for the entire systems. Advanced security technologies will be needed to secure IoT devices and their platforms from data hacking, physical tampering, and new challenges including impersonation and battery-draining denial-of-sleep attacks.

Traditional cryptographic systems, authentication protocols, and safety mechanisms are often insufficient or inadequate due to scalability issues and numerous constraints on system capabilities. The baseline protection must be solid in IoT systems, and the security architecture must be built to withstand long device life cycles, which seems like a difficult task. It's understandable that not all security measures in IoT systems can be effective for such a large population of devices. Therefore, new methodologies and technologies need to be developed in order to meet IoT security, privacy, and reliability requirements (Byres and Lowe, 2004). But it is worthwhile to note that different Internet of Things (IoT) domains are free to set their own security, privacy, and trust standards/protocols. But this factor also leads to the need for standardization of such standards and protocols. As proved by the above discussion, vulnerabilities do exist and can be further discovered in IoT systems that have been in use for a long period of time, such as the Heartbleed bug. The Heartbleed bug suggested that the current standards and mechanisms for security should be checked for weaknesses, vulnerabilities, and loopholes that were overlooked before or were not present earlier. This means we cannot always be sure a system/mechanism is always secure when deployed, used, and integrated with new technologies because new security threats such as malware, security patches, bugs, and system breaches keep on emerging and creating problems with authentication, authorization, privacy, and trust.

Chapter 3

Methodology

The following chapter describes the proposed methodology and research design of the thesis. The chosen qualitative research approach is explained, followed by data collection via interviews during a focus group session. Since data has been collected during the peak of the COVID-19 pandemic, it was quite difficult to motivate people for a separate focus group session followed by individual interviews. Therefore, as described earlier, individual interviews were held during the focus group session and not separately.
Data analysis was performed with grounded theory where patterns in data were highlighted. Lastly, research standards were established along with limitations of the study and ethical considerations during data collection.

3.1 Research Paradigm & Methodology

According to De Villiers (2005, p.3), the paradigm is the primary philosophical point of departure. Whereas Guba and Lincoln (1994, p.105) defined the paradigm as a fundamental belief system. This worldview influences researchers not only in terms of methods, but also on ontological and epistemological levels. It defines the nature of the world and a person's place in it, as well as potential relationships to that world and its components.

Ontology explains what the form and nature of reality is, and what can we learn about our reality or what can be learned? Epistemology is concerned with knowledge, what is known, what is unknown, the relationship between knowledge and the researcher. This methodology also tells us how we can obtain more knowledge. According to Easterby-Smith, et al., (2002), ontology is the assumptions we make about the nature of reality, whereas epistemology is a general set of assumptions about the best ways of inquiring into the nature of the world.

Several methodologies are available within IS research. The choice of single or multiple methodologies depends on different parameters such as topic area, research questions, researcher's background, and the intended respondents. In my case, I will use multiple methodologies (interviews during a focus group session) to lead to stronger validity in my findings.

Information systems research methodology revolves around three key paradigms: positivism, interpretivism, and critical realism. These paradigms are basically intellectual frameworks (ontology and epistemology) embodying a tradition of scientific theories and research.

Out of these three, the interpretivism paradigm is most closely associated with qualitative research, which will be the focal point of my methodology section. The interpretivism paradigm relies on the fact that reality is socially constructed, known as ontology, and it is only understood by interpreting the underlying meaning we give to it, i.e., epistemology (Creswell, 2017).

The interpretivism paradigm is based on studying the views of participants within the search domain. It is conducted via a vast range of questioning techniques in order to extract participants' experiences like interviews, surveys, observations, target groups, etc., a commonly used approach in qualitative research (Creswell, 2017). Because social realities are produced by people through their actions and interactions.

But we also need to understand that social reality cannot be measured objectively, it can only be interpreted by the researcher. Here arises the issue of biasness and un-biasness as the researcher's prior beliefs, values, interests, and assumptions can influence and alter the research interpretations (Creswell, 2017). Therefore, to maintain the credibility, validity, and trustworthiness of research, researchers apply other techniques as well to counter this biasness factor. Figure 10 depicts the research design framework presented by creswell (2017).

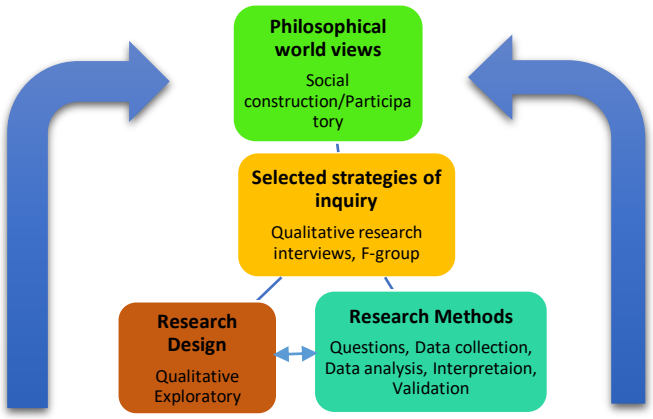


Figure 10: A framework for research design adopted from (Creswell, 2017)

3.2 Research Strategy

Since my fundamental research questions are established and my research purpose and approach are defined. The next step is to chalk out a research strategy, and in the information systems (IS) domain, Franz and Robey (1984) have proposed idiographic rather than nomothetic research strategy, which revolves around examining a particular event, entity, or situation. So I followed an idiographic research strategy since my data collection was during a particular event held at my residential building. Successful execution of this research strategy paves the path for answering the research questions asked by the researchers (saunders, et al., 2009). Rowley (2002) also confirmed that a research strategy should be chosen depending on research questions and the main objectives of the research.

Yin (1994) described five different research strategies to choose from in order to carry out the research process, namely: experiments, surveys, questionnaires, archival analysis, histories, and case studies. According to Weduawatta, et al. (2011), how to select among these strategies depends upon:

- The nature of the research questions (Exploratory, Unstructured in my thesis).
- The extent to which the researcher has control over the natural settings of the participants' environment
- The researcher's focus is on contemporary as compared to historical events.

I had prepared a questionnaire based on the above-defined criteria by (Weduawatta, et al., 2011), where I included open-ended, exploratory questions while engaging with respondents.

The next section explains my research approach and how it should be formulated and executed.

3.3 Research Approach

According to Aaker, Kumar, and Day (2000), research approaches can be categorized into three main categories, namely: exploratory, descriptive, and casual. Since my chosen research paradigm is interpretivism, it is best complemented with exploratory research within qualitative methodologies, because it was conducted to have a better understanding of the existing problem within a chosen segment of people (to understand their knowledge and understanding of IoT devices).

Exploratory research takes a holistic approach and helps to explain the overall nature of the problem, possible decision substitutes, and relevant micro and macro variables to include in the research process (Aaker, Kumar and Day, 2000).

At the same time, qualitative research in information systems must focus on two crucial factors. The first is the technique and standard, and the second is the chosen technique or corresponding theoretical background. Other disciplines must not minimize the importance of information systems (Lee and Liebenau, 1997). After opting for this approach, the researcher can engage in exploring the natural settings of the participants while working with an inductive approach and flexible structure (Creswell, 2017).

3.4 Data Collection & Data Collection Methods

The total number of participants in the study were 10. Out of these 10 participants, seven were men and three were women. Two of the participants were between 30-35, two were between 35-40, two were between 40-45 and one each from between 50-55 and 55-60. I collected and analysed the data in a span of 2-3 weeks around the month of June 2021.

Data collection methods must be compatible with research questions to get correct and realistic results (Harling, 2002). And according to Creswell (2017), while conducting qualitative research studies, the sample should be selected with a predetermined or defined purpose. And the chosen sample must match the purpose and questions of the research being carried out. And they are conveniently reachable for the researcher.

In the case of said thesis, the researcher expected that participants living in his building, i.e., Hosta Hus (https://groenttorvet.dk/hostahus/) have IoT devices at their homes. They are practically using them.

They have little or no prior knowledge of the research problem, and they are willing to respond to my questions raised during a planned focus group session.

Researcher collected the data for the respective research questions in the following way:

- Question 1 (Q 1), a literature review is used as a foundation to define and explain IoT systems, their architecture, their underlying technologies, and their functioning. The goal was to pinpoint key security and privacy risks associated with IoT technology and devices.

- Question 2 (Q2) was investigated through interviews during a focus group session with the target audience being from my building in Valby, Copenhagen.

- Question 3 (Q3) was investigated via reliable online sources, where relevant IT, business, and industrial publications, journals, articles, research papers, theses, and industry leader opinions were examined to find the right answer.

As described in the introduction paragraph of the methodology chapter, primary data collection will be done via semi-structured interviews during a moderated focus group session arranged by the researcher. Since data has been collected during the peak of the COVID-19 pandemic (June 2021), it was quite difficult to motivate people for a separate focus group session. Therefore, to solve this problem, researchers held the individual interviews during the focus group session and not separately. Interviews within focus groups are more efficient when resources such as time and money are limited.

In the section below, I have explained how to conduct interviews and focus group session. Moreover, how is data collected via these two methods?

3.4.1 Semi Structured Open Ended Interviews

One of my primary data collection methods was conducting semi-structured open-ended interviews, given the nature of my research questions (Fontana and Frey, 2005). Minichiello, et al. (1990) defined them as interviews in which questions are kind of predetermined and predefined but are open-ended. They also rely on social interactions between the researcher and the respondents.

Empirical data collection started by conducting interviews which included open-ended questions for the target group chosen from hosta hus (https://groenttorvet.dk/hostahus/). Researcher divided these questions into engagement, exploratory, and exit questions. The objective was to collect information about the main topic and respondents, and evaluate how much the target group knew about the internet of things (IoT), its uses, its disadvantages, its risks, and its potential future use.

Open-ended questions cannot be answered with a simple "yes" or "no", and the interviewee engages in conversation with respondents (Bhattacherjee, 2012).

Probing open-ended questions helped the researcher to get the required information from the respondents (Kvale, 2006). The researcher made sure that his control over the conversation was

minimal, but simultaneously, he encouraged the respondents to relate their personal experiences and perspectives to the current and future use of IoT-based smart home devices (Patton, 2002).
The decision to choose semi-structured interviews as a data collection method depended upon the researcher's epistemology and thesis objectives (Burgess, 1982). It has been observed that researchers using semi-structured interviews often hold a constructivist point of view about social reality and related design studies within an interpretive research paradigm (Denzin, 1989; Robertson and Boyle, 1984).

3.4.1.1 How Data was Collected during Interviews

There is no agreed-upon guideline from researchers on how to conduct a semi-structured interview. Therefore, like others, I followed the following steps (Punch, 1998; Fontana and Frey, 2005):

Step 1- Accessing the interview setting: The researcher must consider the potential political, religious, cultural, and legal barriers. The researcher made sure no sensitive or provoking questions should be asked that involved the respondent's personal choices, such as religious beliefs, dress code, and which political party they supported.

Step 2- Understanding the Surroundings: The researcher must have a strong grasp of his surroundings and what is happening around him/her. The researcher must be familiar with interviewees' backgrounds, language, and culture in order to be successful. Since the session was held in a residential building in the central Copenhagen city area called Valby, all participants were Danes, belonging to different age groups, speaking Danish and behaving like ordinary Danes. The researcher himself spoke Danish with them to make the respondents comfortable and get the best possible information from them.

Step 3- How to present yourself: The researcher must focus on how to present himself/herself as the interview is a two-way conversation, so the researcher's presence must give a sense of comfort. Since the respondents knew the researcher personally, they were quite comfortable while interacting with him. Researchers were also dressed in a normal and casual way to give them a sense of comfort and the feeling that they were also one of them.

Step 4 – Selecting the right interviewee: Because respondents are the primary source of information, the researcher must choose an interviewee who is knowledgeable, willing to participate, and familiar with the local settings. A total of ten people were invited for interviews during the focus group session, and the researchers carefully selected this pool of people that represented all age groups, from young ones to old age. This was done to get a comprehensive picture of their knowledge of the subject matter. And what different age groups think of IoT technology.

Step 5 – Gaining the trust of respondents: is the most crucial step in conducting interviews. The researcher must win the trust of the opponent and make him feel comfortable and confident, especially if the required information is sensitive in nature. The researcher interacted very casually and informally with respondents to gain their trust. Knowing each other previously also played a vital role in establishing the trust factor.

Step 6 - Data collection: can be done by taking notes and memos. But if this method disturbs the flow of conversation, audio recordings can be done as well.

Researchers did take memos during individual interviews to make sure no important information was missed or forgotten. At this point, as a researcher, I kept in mind the challenges associated with this method. The researcher must show the right type and amount of control over conversation (Whyte, 1960).

3.4.2 Focus Groups

In 1991, famous marketing and psychological expert Ernest Dichter introduced the term "Focus Groups.", which means holding a meeting with the selected group of participants to conduct a meaningful discussion and obtain desirable results.

Focus groups are a popular form of qualitative research, where a particular group of people is asked about their perceptions, opinions, beliefs, and attitudes towards a specific product, service, concept, advertisement, idea, or commercial (Morgan, 1998). In my data collection, focus group session facilitated my primary data collection from interviews. A focus group is a group discussion on a particular topic organized by researchers to archive the research purpose. A researcher guides, monitors, and records this discussion, so it is not diverted from the topic (Kitzinger, 1994).

This practice gives valuable insights into what motivates and triggers the attention of participants. And with a cooperative and collaborative outlook, focus groups encourage participants to speak about what's on their minds regarding the topic and give their share of feedback.

3.4.2.1 Components of a Focus Group

Generally, focus groups consist of the following two components:

Participants - The very first and most important step in conducting focus group research is the process of participant/respondent selection. The researcher paid extra attention while recruiting participants/respondents. Researcher anticipated that respondents have the necessary knowledge about the research topic, so they can add value to the conversation.

A total of ten respondents participated in the data collection process. Researchers found out that people were reluctant to have physical contact and were not very eager to participate in longer or boring sessions. So my aim was to keep it short, precise, and to the point and ask only relevant questions. Let the respondents express themselves, and only interfere when I felt they were diverting too much from the main topic.

Respondents were chosen very carefully and the age diversity factor was kept in mind during the selection process. The aim was to get responses on security and privacy issues from all age groups to establish a better understanding of the phenomenon. The youngest respondents were between 30ys and 35y, whereas the oldest ones were between 55y and 60y.

The researcher - acted as a moderator or facilitator in this process. The researcher did his best to be unbiased and partial during the study to maintain the validity and reliability of the session.

3.4.2.2 How Focus Group Session was Conducted

As explained earlier, due to the corona crisis and limited availability of respondents, researchers conducted focus group sessions and interviews simultaneously at the same place. A total of ten respondents participated in the focus group sessions and interviews. They were all residents of Hosta Hus, where the researcher lives.

Researcher encouraged people to engage in group discussions or express their personal knowledge and experiences when a question was asked of a particular respondent. So when the researcher asked a question to Respondent 1, after his answers, other respondents also shared their answers to the same question, leading to meaningful discussions on a number of occasions.

Bloor, Frankland, Thomas and Robson (2001) suggested the following steps to conduct a focus group session: The researcher carefully chose the participants for the study and presented them as a true reflection of his target population. The researcher had a clear plan for his focus group session. When the focus group goals were defined, the researcher started formulating his questions. The focus group was held physically in the common hall designated for such activities in the researchers' residential building (https://groenttorvet.dk/hostahus/). My focus group session consisted of 10 members.

The researcher made sure that the place was convenient and comfortable for participants. The researcher produced an information brochure and forum posts with a welcome note, agenda, and overall rules of the discussion for the smooth flow of the event later on. This information was posted on the social media group building (https://www.facebook.com/groups/2646909905396407).

A focus group session of 1-2:30 hours was conducted. Participants were greeted and thanked for coming and taking part in the discussion. The quick agenda of the session was announced, then formal goals and rules of the session were set and explained to selected participants. Researchers made sure that all participants got a fair chance to express their opinion on particular questions and got a chance to be heard.

The questionnaire was confined to 30-32 questions maximum. The researcher started with "engagement questions" to introduce himself to participants, although they directly or indirectly knew the researcher, then made them comfortable by socializing with them.

In the next phase, researchers moved to more "exploratory questions" to get an idea of what kind of IoT devices respondents were using, what their familiarity level was, how these devices were helping them in their daily lives, and how much they were aware of their personal privacy and security. The session ended with "exit questions", to make sure researchers hadn't missed any important information that could have helped in data analysis later on.

3.5 Data Analysis

Thesis's theoretical background, research methodology, and supervisor suggested that I can implement a grounded theory with an inductive approach to my collected data in order to develop novel points out of the data and to highlight re-occurring themes to understand what data is saying.

3.5.1 Grounded Theory

According to Glaser (1992), grounded theory is both a process and an outcome, and to better understand the mechanisms of grounded theory, and how to generate meaningful insights out of it, we need to employ it on data itself and not to consider it as a theory. As Urquhart and Fernández (2016) pointed out, grounded theory is particularly useful when there are no previous theories in the research area. In the case of my thesis, there is not a specific theory that can be directly related to the security and privacy issues of IoT and smart devices. Orlikowski (1993) claims, when it comes to investigating processes and improvements, grounded theory is a perfect match. Wiesche, et al. (2017) argue that in IS research, grounded theory is often used to investigate technological changes and socio-technical activities in new research domains.

Moreover, researchers concluded that the use of grounded theory is highly dependent on contextual variables such as the research's location and length. Grounded theory can provide a range of coding and data analysis approaches that are well suited to the interpretive approach since it keeps data and analysis close to each other for inductive discoveries (Hughes and Jones, 2003).

Birks, et al. (2013) argue that grounded theory can handle a spectrum of different viewpoints, and its adaptability and flexibility are its most valuable features. But at the same time, researchers need to be very careful when dealing with the flexibility factor, because a new or inexperienced researcher can find it difficult to implement it and draw the required results.

Keeping this factor in mind, I opted for open coding instead of axial coding. Later, they will be linked to each other to create general categories. These categories will make it simpler for the audience to understand the answers collected from interviews during a focus group. These will also help me to observe and understand patterns in collected data. We can then move on to selective codes to base our theory or novel points on.

Moving on to the inductive approach within grounded theory, it is a way of thinking about analysis as coined by (Strauss, 1991). Researchers in the inductive approach use open-ended methods to develop findings. Therefore, while applying the inductive approach, we must deal with data as open-mindedly as possible, immerse ourselves in data, look for trends and patterns, define key variables, and then progressively develop thorough explanations of findings.

Grounded theory, in the point of view of Glaser (1992), is not about the form of data but rather how researchers approach data analysis and interpretations. As a result, the data to be evaluated may be qualitative, quantitative, or a combination of the two (Glaser, 1992; Glaser and Strauss, 1967).

3.5.1.1 How Grounded Theory is Applied on Collected Data

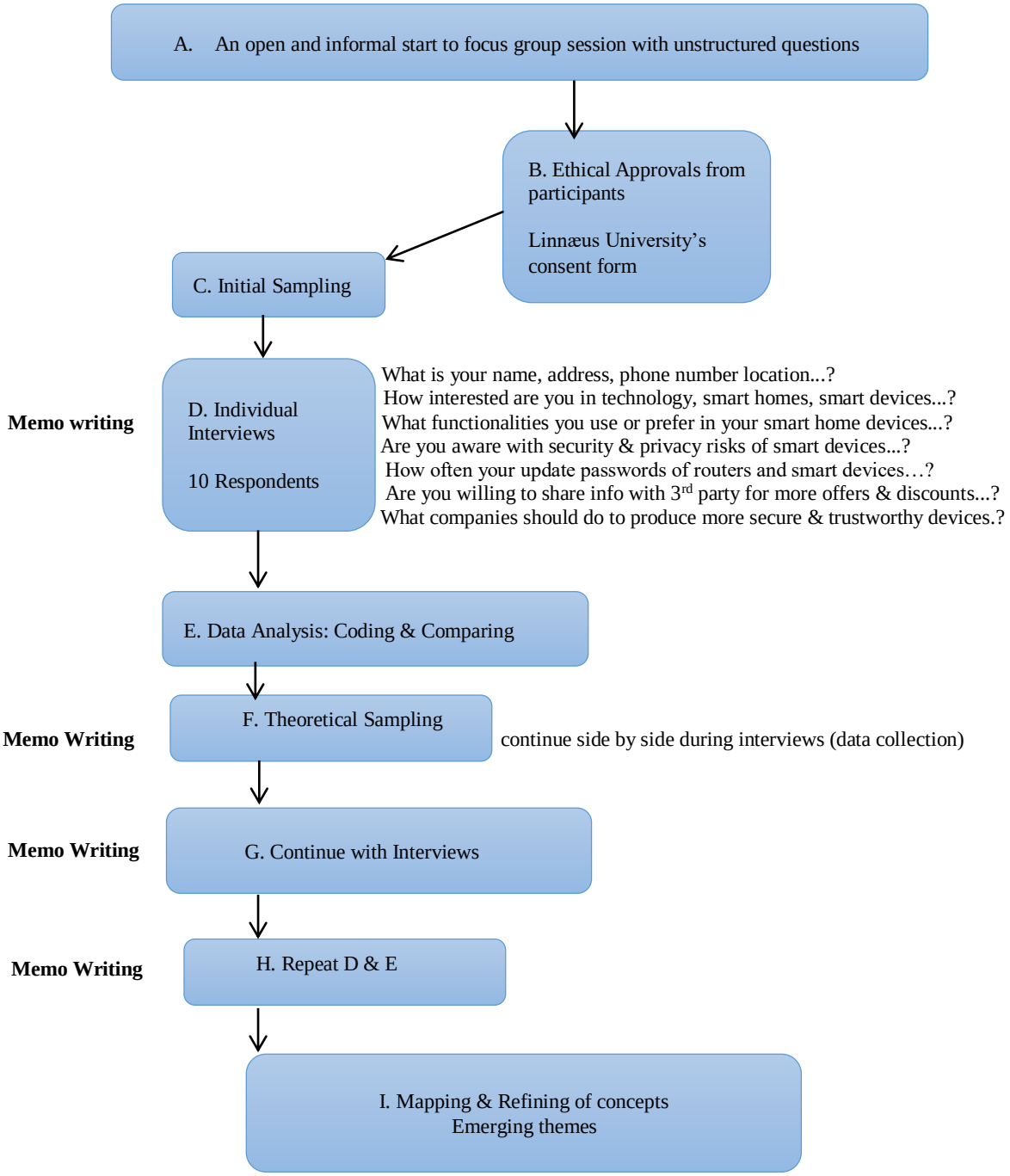


Figure 11: How to apply grounded theory principles on data (Author's contribution)

Figure 11 above shows the step by step approach taken to apply grounded theory to data. Each step is explained in detail below.

The researchers in a grounded theory study should not wait until the entire data is obtained and then start to analyze it. To allow theoretical sampling in a grounded theory study, researchers must begin as soon as possible and continue in parallel with data collection.

3.5.1.1.1 Interview Questions

Grounded theory experiments are typically concerned with social processes or behaviours, asking what happens and how people communicate and interpret. Grounded theory research starts with open questions, the same approach I followed in my interviews and started discussion with open ended semi structured questions about respondents' personal information (name, address, gender, phone number etc.) and their general attitude towards technology. At this point, I assumed that I don't know anything about the interpretations that can influence participants' behaviours.

Questions for interviews were divided into three distinct sections:

- Engagement Questions - Respondents' personal information and socializing etc.
- Exploratory Questions - General information and understanding about technology, smart homes, and the Internet of things (IoT), actual and perceived usage of IoT devices, advantages and disadvantages of IoT devices, security and privacy challenges, and level of understanding about them.
- Exit Questions - Willingness to buy again, shift towards technology, what companies should do, and what things they believe should be kept in mind while buying, using, and disposing of IoT devices.

3.5.1.1.2 Ethical Approvals

Ethical approvals are explained in detail in section 3.8 of the methodology chapter.

3.5.1.1.3 Initial Sampling & Theoretical Sampling

Collected data was used for initial sampling and later for theoretical sampling (Appendix 2). Researcher prepared the transcripts of the collected data from individual respondents.

3.5.1.1.4 Coding & Comparing

The development of a grounded theory requires coding. Coding is the crucial bridge between gathering data and formulating an emergent theory to explain it. With the help of coding, I can explain what data is saying and can play with it to extract meaning out of it. Coding can be divided into different phases.

For instance, in early or initial coding, I had the liberty to produce different meanings or ideas inductively from the data, such as respondents' age diversity, their understanding of technology, and their familiarity with concepts of smart homes and devices.

Then comes focus coding, where I focused on a chosen set of main codes from the study. This generally requires deciding which initial codes are the most common or significant, and which contribute the

most to the analysis. Then, in theoretical coding, I refined my theory's final categories and linked them together. At this point, my goal was to keep the codes as similar to the data as possible.

After my introductory questions from the focus group session, I had considerable data available with initial codes, including respondents' personal information, technology awareness, tech savviness, and knowledge about security and privacy. Then I decided to generate my focus codes from data gained by asking questions about respondents' use of IoT devices, what usability of IoT devices is important to them, how many devices they have at home, the availability of routers, how often they update passwords, and knowledge about these devices spying on them.

Following the comparative method in grounded theory, I compared codes with codes and data with data, thus enabling me to understand the relationship between them. This step also helped me to produce my theoretical codes and make sense of the data to develop my knowledge about the security and privacy awareness of respondents (Appendix 2).

3.5.1.1.5 Mapping & Refining of Concepts

After theoretical sampling, researcher begin coding theoretically to identify core categories or themes. This phase is termed as theoretical saturation.

Theoretical saturation revealed certain core categories, including the six most common categories from the participant responses. Similarities in respondents' responses were used to develop core categories. For instance, responses to initial questions were categorized under personal information, responses to exploratory questions were categorized under other core categories and so on.

Emerging patterns were further narrowed down to the most common ones, which were then classified in order of occurrence. E.g. use of technology, smart homes and devices, smart devices as a comfort factor and an improvement in quality of life, ordinary security resilience, lack of true security and privacy awareness, 3rd party involvement, what device manufacturers should do and willingness to buy again.

How different phases of grounded theory are executed can be seen in Appendix 3.

3.6 Research Standards

Academic research standards are a set of ethical guidelines that researchers must follow when doing and reporting research. It asks questions such as whether the research question is valid for the desired outcome, whether the methodology chosen is appropriate for addressing the research question, whether the research design is appropriate for the methodology, whether the sampling and data analysis is appropriate, and whether the findings and conclusions are valid for the sample and context.

A logical sequence of statements is anticipated to emerge from a particular research process. Yin (1994) presented four techniques to examine the quality of the research process, namely: construct validity, internal validity, external validity, and reliability. He also suggested two ways to improve the study's construct validity:

1. collect data from various sources. (primary and secondary data sources).

2. build a chain of evidence by ensuring continuity, flow, and sequence during the data collection process. For research purposes, the entire process may be supervised by a designated supervisor.

To ensure construct validity, researchers collected data from (focus group discussion and semi-structured open-ended interviews) and (university library databases, reputed journals, research and conference papers, industrial publications, and leading consultancy firm reports). To establish a chain of evidence, the thesis report is being supervised and reviewed by a designated supervisor from the university, i.e., Prof. David Randall.

Remaining within my exploratory research parameters, I focused on establishing the internal and external validity of my thesis report. Internal validity is something that is only relevant to the specific study in question, like in the case of my thesis, it is to access people's knowledge and understanding of the IoT devices they use. Internal validity deals with the establishment of connections between the study's variables.

Data for my research report was gathered from a variety of sources, both primary and secondary sources. When the interviewing process was documented, I cross-checked the information provided by the respondents with the recorded transcripts and memos.

Secondary data sources were verified by answering questions like: Who collected the data? (researcher), What is the purpose of this data collection? (to answer research questions about IoT usage and security/privacy), When was the data collected (between Jan 2021 and July 2021)? How was the data collected? (university databases and online sources) and whether the data is consistent with data from other sources? The researcher created a logical flow between data collection and analysis methods, so a reader of this thesis can understand the outcome without any confusion.

Moving on to external validity, which refers to the degree to which the results of research can be applied to other cases, individuals, settings, and measures (Rodgers and Cowles, 1993). In other words, external validity refers to how generalizable the findings are. It can be difficult to achieve high levels of external validity for primary data in my thesis, because people who are interviewed may lie or provide incorrect and misleading information about their perception and use of IoT devices and knowledge about security/privacy concerns.

In the end, a reliability test in quantitative research refers to the methods and outcomes being able to be exactly replicated (Grossoehme, 2014).

Researcher used the concept of reliability in my thesis report to reduce the risk of errors in research and biasness of respondents during interviews and focus group discussion. To achieve higher reliability from respondents, I carefully selected the respondents I could trust to have the right information and who were willing to co-operate and share the required information (Silverman, 2009). The figure 12 below shows how validity and reliability can be established in a research process.

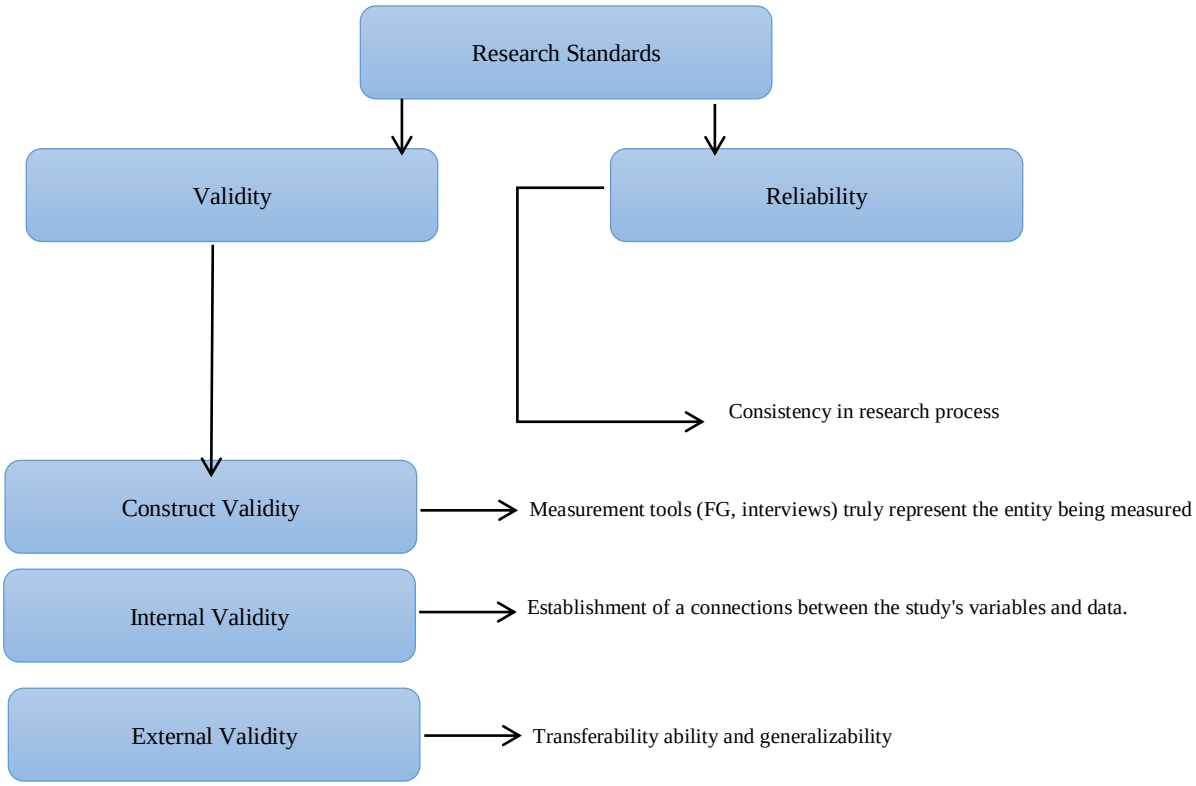


Figure 12: Validity and Reliability criteria in the research process (Author's contribution)

3.7 Limitations of the Study

Collecting, compiling, organizing, and interpreting qualitative data is also an issue and requires a certain set of competencies. Just because of the sheer nature of this data, the researcher has to go through each individual respondent to form a more comprehensive understanding of why these participants felt or reacted to certain questions in a particular or unique way.

And since information or data is often descriptive rather than numerical/statistical, preparing the result is more time-intensive and requires concentration. Then arises the question of biasness either from the respondent's side or researcher's side, towards certain situations or questions in the interviews, because sometimes researchers' presence might contribute to biased responses from the respondents. (Creswell, 2017). Therefore, the quality of research depends on the researcher's un-biasness.

My goal was to avoid or minimize "design errors" (Iacobucci and Churchill, 2018), because these errors trigger a number of other errors that ultimately destroy the validity and reliability of the whole research process.

Finally, due to the COVID-19 Pandemic, people were reluctant to give information in physical meetings. That is why I had to go with a small focus group session during which interviews were also conducted. Then, due to the lockdown and other precautionary measures in place, people might not be interested in providing their opinions as stress and anxiety levels were higher than normal at that moment.

3.8 Ethical Considerations

My research involves gathering, analyzing, and storing personal information about individuals who have responded to my questions during interviews and focus group discussion and during such studies, respondents are often concerned about their identity or personal information. To ensure privacy, I did not request information that could be used to directly identify a specific person, such as names, email addresses, home addresses, and phone numbers.

A genuine effort was made to maintain confidentiality. And where individuals are mentioned, instead of mentioning their names, they are described as respondents 1, 2, and so on. Since the subject matter of my thesis is privacy and security, therefore, managing personal information was a critical component of the thesis report. The consent form template provided by the course coordinator was printed and distributed to the respondents, which was duly signed by them. One example is attached in the appendix section.

Participants were briefed about the study's intent and nature prior to participation, and they were given the option to withdraw from the interviews if they felt uncomfortable.

Chapter 4

Empirical Findings

The following chapter presents the results of the focus group and interviews in a synthesized manner, pointing to commonalities and differences in respondents' answers. Focus group sessions and interviews were held at the same time with a selected group of respondents. A total of 33 questions were asked of respondents individually, and their responses were documented and analysed. Cross communication among respondents was encouraged to justify the focus group session.

4.1 Data Collection from Interviews

To evaluate the general public's knowledge, level of understanding, interaction with IoT technology, current and intended use, I conducted interviews during a focus group session with ten respondents chosen from my neighbourhood (Appendix 1). Results are shown below:

Table 4

What is your Age?

	Age	No of Respondents
	30y-35y	2
	35y-40y	2
	40y-45y	2
	45y-50y	2
	50y-55y	1
	55y-60y	1

As shown in the above table, the total number of participants in the study were 10. Two of them were between 30-35, two were between 35-40, two were between 40-45 and one each was between 50-55 and 55-60.

Table 5 What is your Gender?		
	Male	**Female**
	7	3

Out of these 10 participants, seven were men and three were women.

Table 6 How much interested are you in technology?			
	Very Interested	**Little Interested**	**Not Interested**
	6	2	2

Out of 10 respondents, 6 were very much interested in using technology in their home appliances and daily life. They fall into the age group of 30–45, so it is evident that relatively young people are more interested in technology and modern day gadgets. 2 middle age participants were also interested in technology but not very excited or enthusiastic about it, whereas 2 old age respondents were not interested at all.

Table 7 Have you heard about term smart homes or smart home devices...?		
	Yes	**No**
	9	1

Almost everybody had heard about the term smart homes and smart home devices except one elderly lady, who was neither interested in technology nor heard about these terminologies.

Table 8 If yes, what comes into your mind ...?		
	Usability	**No of Respondents**
	Smart heating	10
	Intelligent virtual assistants (Alexa, Google assistant etc.)	6
	Smart lighting	6
	Useful information (weather, traffic)	7
	Alarms	7
	Smart appliances (fridge, speakers, Tv)	7
	Health & fitness gadgets	7

All respondents knew about heating systems, as it was a built-in functionality in their homes, which were newly constructed. Six respondents were familiar with virtual assistants like Alexa, Google Assistant, and others. 4 people didn't know about smart virtual assistants.

Six respondents were familiar with smart lighting systems like Philips Hue and Lifx. Seven thought it was a good idea to be aware of local weather and traffic conditions in order to plan outdoor activities and dress appropriately. Then come smart home appliances like TVs, fridges, vacuum cleaners, and music systems. Home security and home alarms were also mentioned in reasonable numbers. Seven people were familiar with the connection between smart phones and health/fitness gadgets, especially young respondents.

Table 9

How many smart devices do you have at home...?

	Respondents	No of Devices
	30y-35y	4
	35y-40y	4
	40y-45y	3
	45y-50y	3
	50y-55y	1
	55y-60y	1

It can be seen from the table above that young people tend to have more devices and gadgets at home as compared to older age brackets. People between the ages of 30 and 45, on average, have four devices and gadgets that they use on a daily basis. Middle-aged and elderly respondents did have routers and a few other devices but were not tech savvy.

Table 10

Do you have Alexa, Siri, Google Assistant or other virtual assistants at home...?

	Virtual Assistants	No of Respondents
	Alexa	3
	Google Assistant	3
	Siri	0
	Cortana	0
	Bixby	0

Multiple virtual assistants were used by respondents. Amazon's Alexa and Google assistant turned out to be the most popular virtual assistants as each was used by three respondents. Cortana from Microsoft and Bixby from Samsung were not popular among respondents.

Table 11 What services or functions, you use from your IoT devices...?		
	Functions	**No of Respondents**
	Energy savings	10
	Ambiance lighting	8
	Listening music	9
	Weather updates	10
	Smart locks	7
	Setting alarms	6
	Maximizing home security	7
	Health & fitness updates	5

When participants were asked about: what they use IoT devices/smart home devices for, or what comfort and functionalities they are expecting... The answers were very different, reflecting the age group they were representing. Nearly all participants were interested in reducing their energy bills and saving money. The second most popular use turned out to be playing music and controlling lights via virtual assistants like (Alexa, Google, etc.). Participants were also very interested in weather forecasts and traffic updates, since living in Scandinavia and knowing about the weather is very important for planning your daily activities.

Respondent 5 (45-50 yrs.):" reducing my heating bill, which is quite expensive in Denmark. I use a smart lock system which I can control from my smartphone. ".
Respondent 6 (aged 50–55)"For me, the important thing is to save some money on these things and bring some comfort in life. I am happy to use these smart home speakers that "listen to me".
Respondent 4 (aged 35-40): "I listen to music and I use Alexa for weather and traffic updates when I am going out".
Respondent 3 (30-35 yrs.) "better quality of life", "more health and fitness conscious", "simpler and easier everyday life" and "smart home appliances".
Respondent 9 (55-60 yrs.): "my TV is smart, I have a remote vacuum cleaner, and a few smart functions in my fridge".

Participants ranked home security or remote home security very high, with nearly seven out of ten participants mentioning it. They were interested in remote Wi-Fi cameras, smart home alarms, and smart door locks that can be controlled via applications on their smartphones. A considerable number of participants also use smartwatches from Apple, Samsung, and Huawei for tracking their health and fitness.

Table 12 Do you have a router at home...?		
	Yes	**No**
	10	0

As shown in the table above, all ten respondents have routers at home. These routers are of different types. Mostly using a high-speed router with a speed limit of up to 1000 MBPS. Most of the respondents were using "mesh networks". Surprisingly, middle-aged respondents or older ones were also using them. But they also mentioned that they took the help of family members to set up the networks.

Table 13

Do you update your router setting regularly...?

	Yes	No
	7	3

Seven out of ten respondents mention that they regularly update their router settings when prompted by a device or they themselves keep an eye on them. Whereas three respondents don't update them regularly, mostly middle-aged or older respondents fall into this bracket. The reason was that they were unable to do so, or it was difficult for them to remember passwords all the time.

Participants, mainly those aged 40-60, were not aware of the consequences of having weak router passwords, like if hackers cracked their passwords, they could gain access to their social media accounts, bank accounts, emails, and other sensitive accounts that contain their personal information. And they can become a victim of identity theft.

Respondent 5 (45-50 yrs.): "I use a normal password. I am not interested in updating regularly. "
Respondent 6 (50-55 yrs.) "I have normal passwords. I don't update them often. "I keep all my passwords in a single application".
Respondent 4 (35-40)"I usually keep strong passwords and update them regularly".
Respondent 3 (30–35 yrs.) "I use strong passwords and normally update them periodically".
Respondent 9 (55-60 yrs.): "my password is very normal because it is difficult for me to remember a difficult one".

Table 14

Questions about router Passwords...?

	Questions	No of Respondents
	Have you changed the default password	10
	We often change default password	8
	Didn't change default password	0
	Took help to change default password	2
	Change default password every 3 months	3
	Change default password every 6 months	7
	We use strong password for router	7
	We use weak password for router	3

When I asked them questions about router passwords. Their answers were very diverse and interesting. There was not a single person who hadn't changed their default password since they got the device. Eight people changed and updated their passwords. Out of those eight six of them regularly changed their passwords and followed password instruction to create a strong password. Two people, mostly middle and old age, took help to change their passwords because the application was too complicated and they could not do it themselves. And lastly, 3 people turned out to be more conscious mainly of young respondents and update their password every 3 months. They use" password vaults"-applications provided by different companies to secure their passwords.

Table 15

Why you have purchased smart devices...?

	Reasons	No of Respondents
	build in (smart floor heating)	10
	To bring comfort in daily life	9
	to follow technology trend	7
	positive feedback from friends & relatives	8
	to give home a modern look	5
	security purposes (alarms)	6
	to follow more healthy lifestyle	5
	to reduces light & heating bills	9
	no specific reason	1

The answer to this question was very crucial for determining the general perception and behaviour of people and what made them buy these IoT or smart devices. 10 out of ten respondents had some built-in smart devices in their homes, because they lived in a relatively modern and newly built neighbourhood that had some state-of-the-art features such as (smart floor heating, smart climate control, smart lighting etc.). Nine people believed it would definitely improve their daily life routines. Seven believe they are just following the technology transformation and trends. Eight believed they were forced to buy them when they heard positive feedback from their social circle (friends, family, colleagues). Nine believed they could reduce their energy costs and consumption by doing so. Five thought it would improve their health by monitoring it via smart watches or different apps on their smartphones. One person remained neutral and didn't mention any specific reason, belonging to the old age bracket.

Table 16

How much marketing & advertising Effected your decision...?

	to great extent	to some extent	not at all
	8	2	0

When participants were asked about: who influenced them to buy IoT devices and how much advertising and marketing affected their decision making...? In answer, family members and friends

turned out to be the main reasons for buying smart home devices. A considerable number of participants, 5-8 from all age groups, said that their close family members were already using smart home appliances/devices and they explained their benefits and comforts for everyday life. But advertising and marketing on different social media platforms like Facebook, Instagram, Twitter, YouTube, and blogs also forced them to think about buying or using these devices.

Nearly every single participant said that when they are using social media and intentionally or unintentionally clicking on smart home device ads, they make cookies on that platform or website to remember their preferences and choices. And then over a certain period of time, they were bombarded with the same ads again and again. which eventually forced them to buy these devices.

Respondent 5 (45-50 yrs.): "my close family member forced me to buy something smart".

Respondent 6 (aged 50–55)"I got it as a gift to make my life a bit more comfortable".

Respondent 8 (35-40 yrs.) "I see ads all the time on my Facebook wall".

Respondent 3 (30-35 yrs.) & Respondent 4 (35-40 yrs.) "I got positive reviews from my friends", "social media influenced me a lot, in fact, almost forced me", "TV ads made me buy one" and "weekly ads magazine made my mind," as I follow that magazine regularly."

Respondent 9 (55-60 yrs.): "I was not affected by these things; few things were already in my apartment when I moved in".

Following suit, built-in smart features in homes and upgrades from legacy systems were cited as reasons for opting for smart home devices. Furthermore, 8 participants said that the influence of technology is impossible to ignore and social media provides them with new channels to communicate with different device manufacturers and brands, thus making decision-making easier.

Table 17

How difficult or complicated these devices are to use ...?

	quite complicated	little bit complicated	not at all
	6	3	1

Out of ten, six people experienced that these IoT devices are quite complicated to use. These six included all age groups. Three thought they were easy to understand and use. They were mainly between 30 and 40 years old. One respondent, who was basically working in the IT industry, found them to be very easy to use.

Table 18

Are you aware about the security & privacy risks associated with IoT devices...?

	Yes, we know	Yes, but don't know exactly what risks	No idea
	4	5	1

Five people do understand that there are risks associated with smart or IoT devices, but they are not aware of exactly what type of risks there are. (identity theft, personal info theft, financial info theft, or something else). Four people had a relatively better understanding of the risks, but they were still unaware of the complete picture. Whereas, one person had no idea at all.
In general, participants were aware of privacy and security issues associated with IoT devices. But they were not sure to what extent either these devices or the wrong people through these devices could exploit their privacy. and can hack their personal, financial, and other sensitive information such as likes and dislikes, daily routines, etc. On average, 5-8 participants in the age group of 30-50 yrs. were aware of privacy and security risks but were not sure that this issue could really hurt them severely.

Older participants, 50-60 yrs., were unaware of the threat almost completely. They didn't know that hackers or criminal-minded people can really misuse their information and data, as each connected device in their home notifies its corresponding application in smartphones when it's being used, sending a digital fingerprint to the router. and hackers spying on their routers can learn about their daily schedule and can view videos/images of them or maps of their home for any future criminal activity.

Those participants who were conscious about hacking while discussing privacy and security breaches used phrases like online hacking, information in the wrong hands, information theft and criminals may try to take control. But despite this, they have not expressed serious reservations over the device manufacturers' commercial use of their data.

When participants were asked to identify potential threats to their privacy and security, keeping in mind previous responses, participants did not reply with different answers but instead built on their earlier reflections and point of view about privacy and security in the context of general threats.

Respondent 5 (45-50 yrs.): "I know privacy and security is an issue but don't know how much".
Respondent 6 (50-55 yrs.): "Sometimes I fear my personal information can be leaked or hacked because I don't know how to properly use it."
Respondent 4 (aged 35-40)"I do believe privacy and security is a serious issue, but I am not sure how much information these devices can collect or steal."
Respondent 3 (30–35 yrs.) "It is a serious issue, but I can't say how much".
Respondent 9 (55-60 yrs.): "I have no idea".

Table 19

**Do you know IoT devices collect info about you ...?
(address, phone no, email, passwords, location)**

	Yes	No	No idea
	6	3	1

Six respondents did acknowledge that they knew smart devices collected information about them but were not sure to what extent and what type of information. Three didn't know about it, and one elderly person even didn't know that these devices had the capability to collect information about them.

Table 20 Do you know, your IoT devices can record your daily routine, likes/dislikes, choices etc...?			
	Yes	**No**	**Didn't think about it**
	2	7	1

Besides knowing that these smart devices can have information about them, Seven people didn't have the idea that these smart devices could spy on them. can monitor their routine, eating, browsing, and driving habits. Only two tech savvy people knew about it and one person didn't think about it.

Table 21 Do you know, your IoT devices can spy on you...? (by microphones, cameras, sensors)			
	Yes	**No**	**Didn't think about it**
	1	7	2

When I asked them about the technical details of these devices, Seven people were not fully sure that they knew they could be spied on by their home devices or appliances. Three didn't think too much, because of their busy daily routines and only one tech savvy IT guy completely knew about it.

Table 22 Do you know, your personal information can go in wrong hands...?			
	Yes	**No**	**Didn't think about it**
	2	6	2

Six people had no idea about it. 2 people said. Yes, they knew about it. and two people didn't think about it.

Table 23 What information can go in wrong hands...?		
	Information	**No of Respondents**
	financial info	2
	personal info	6
	location	2

Most of the respondents were worried about their personal information going in the wrong hands. Two of them were not happy that their personal location is disclosed to others and that can be misused. Two were afraid that their money matters could be revealed to unauthorized people.

Furthermore, participants mentioned that fear of being recorded without knowing, social media spying, access to financial info, devices storing, transmitting, and using their personal data without permission, devices doing things they weren't supposed to do, gathering voice and image data, obtaining credit card information, whereabouts (e.g., whether a person is at home or not, what time a person comes/what time they leave), and medical/health data were also worrying factors for them.

Table 24

Have you ever been hacked, accidently downloaded malware or installed new software without consent...?

	Yes	No	Don't Know
	6	2	2

Six people believed that they had willingly or unwillingly become victims of these cyber-attacks. Two didn't face any major threats. whereas the other two didn't think about it.

Young people aged 30-45 reported unknowingly downloading browsers hidden in free software (one person cited CCleaner as an example, saying that when he installed free software for PC cleaning, their browser was also installed unwillingly and without their knowledge). Couple of participants mentioned about getting scam emails from Nigeria, Mali, and South Africa. In one case, a participant even got a phone call from India, where a person was asking for remote access to his laptop, claiming to be from Microsoft, and saying that his workstation needed some critical Windows updates.

Table 25

Did you read the purchase agreement or privacy policy when buying these devices...?

	Yes	No	Didn't think about it
	1	6	3

Six people didn't consider it at all when they were buying their smart watches, Tvs or virtual assistants. One IT guy did read the purchase agreement and before saying yes to everything, checked what information they would have access to when they started using the device. Three people didn't bother to take it as an issue.

Table 26

Are you willing to provide more personal data if you are offered things in return e.g. special deals, discounts etc...?

	Yes	No	Didn't think about it
	2	7	1

Seven people out of ten replied with a no. They were not moved by these marketing scams whereas two people were partially willing to share their information and one didn't think about it.

When participants had to elaborate if they would be willing to share personal data to make the price for standard service cheaper or to avail other benefits like value-added services, add free content, extra features in exchange of data with device manufacturers or 3rd party vendors. Most of the participants refused to share their personal data, except for an older group who seemed to be interested in these deals. Only 2-3 out of ten participants identified privacy and security risks associated with 3rd party data collection. The majority of participants see threats in the form of hacking, information leakage, and other types of attacks. The intriguing thing was that no one expressed serious concerns about how companies, their local or federal government might use the data collected from them.

Respondent 5 (45-50 yrs.): "I won't share my data for marketing and advertising purposes".
Respondent 6 (50-55 yrs.): "I can share some information if I get some benefits, like a discount".
Respondent 4 (35-40 yrs.): "No, this does not appeal to me."
Respondent 3 (30-35 yrs.) "in fact, I see it as a security issue".
Respondent 9 (55-60 yrs.): "I don't know" or "didn't think about it"

Participants drew a thin line between data privacy and security and allowing certain types of data. One participant stated that data collection is common practice for businesses, citing smart lighting as an example. If data is not obtained, it is impossible to know how long the light has been on. He was fine with data collection in this situation, but not if the device manufacturer planned to use it for targeted ads or sell it to 3rd parties. Based on the responses, we can say that there is a fine line between data collection and privacy violation. Participants wanted more convenience and comfort, but their anonymity or privacy would be jeopardized if they did so, so they were ignored.

Table 27

Have you changed the password of your IoT devices/gadgets in past 6 months...?

	Yes	No	Didn't think about it
	3	5	2

When it comes to Wi-Fi passwords, only the younger age group of 30-45 yrs. were using strong passwords and updating them every six months or when prompted by the device itself. They were using "password vault" apps like NordPass, 1password, and Last pass to store their passwords.
Five people didn't change their passwords that often on their smart devices. Only three did, and two didn't think about it so seriously.

Table 28

Do you use the same password for all devices and gadgets...?

	Yes	No	Didn't think about it
	3	7	0

Seven respondents were using different passwords for their different devices, but as it is difficult to remember so many passwords simultaneously, They were using "password vaults" offered by different companies to keep all of their passwords in the same place. They were using one master password to access that vault. Three people used the same password for all of their devices, including the elderly.

Table 29 Do you timely update, versions of your devices when prompted...?			
	Yes	**No**	**Didn't think about it**
	1	6	3

Six people didn't update or only updated when it was mandatory to use the product. They said some features are free, or don't work, or start giving error messages if not updated when prompted. So sometimes they have to update in order to use the product. Otherwise, they were not interested due to a lack of time and interest. Our one tech savvy person does update all devices regularly to use them effectively. Whereas, three people were not interested.

Table 30 What device/ gadget manufacturers should do to make them more secure...?		
	Answers	**No of Respondents**
	Ask permission before giving info to 3rd party	8
	More secure back end data solutions	3
	Clearly define what information will be kept	6
	Clearly define data policy	7
	Product or service improvements	7
	Regular updates	6
	Good customer service	9
	Easy installation	8
	User friendly	10
	More secure devices	10

Ten out of ten agreed that the usability and security of these smart devices and gadgets are their top priorities. Respondents said they have different abilities or knowledge about technology and the use of these devices, so it is very important for them to be able to navigate through them and to be able to use their functions.

The second most important factor was customer satisfaction, so if something happens or they are unable to use their product, there must be a friendly person at the help desk to help them. Respondents were also giving attention to their personal data, i.e., how their data would be kept and used. They didn't want it to be used for social media marketing, email marketing or direct marketing. Respondents also gave importance to the ethical considerations that companies must consider, while selling them products. Then there must not be any hidden terms and conditions involved.

Table 31 Are you satisfied with the products offered by manufacturers...?			
	Yes	**No**	**Didn't think about it**
	7	2	1

Most of the respondents were generally satisfied with the smart devices they were using in their homes, especially smart climate control, smart lighting, and virtual assistants. One respondent was not satisfied as he found them difficult to operate. Whereas, they were neutral about their experiences.

collecting data to enhance services but sharing personally identifiable data with third parties. Big corporations like Facebook, Microsoft, and Google know all about you. Is Alexa collecting everything I say for Amazon's benefit? Does Google know more about us than we do? These concerns were mentioned by 5 out of 10 participants. These responses indicate that participants were aware that device manufacturers have a role to play in data privacy and protection. Even so, participants were not entirely clear on the topic.

Table 32 Based on your experience so far , would you like to buy a smart device again ...?			
	Yes	**No**	**Didn't think about it**
	7	2	1

Efficiency, lower utility bills, convenience, comfort, intelligence, virtual assistants, home alarms, and light customization according to need were the factors highlighted by participants for buying and using smart home devices/IoT devices.

Generally, respondents were overall satisfied with the products and services they were offered, as far as usability or functionality was concerned. Respondents also believed this is where the future is heading. But they were not satisfied with the security and information/data policy of device manufacturers. Because they didn't know what information was stored and further used by these companies themselves, by government departments and by 3rd parties. One person was unsure about whether he would buy them again in the future or not. From the response to this question, it is evident that the majority will buy these devices again.

4.2 Data Collection from Focus Group Session

Since interviews were held within the focus group session and not separately, So it was a challenge for researcher to transcript and analyse data separately for both methods.

To overcome this problem, researcher encouraged cross-communication between respondents and promoted group discussion when a particular respondent asked a question on a specific issue. Respondents were encouraged to unpack more information and express their views more openly. The focus group consisted of the same 10 people who were individually interviewed. The length of the focus group session was 2:30 hours maximum and was held in the common room within the Hosta Hus building where the researchers and respondents reside.

Interactions during the session were open-ended, informal, semi-structured, and based on the primary research questions. For instance, when I presented a question to a particular respondent and the conversation had started, I asked sub-questions to leverage discussion among respondents, e.g., what do you think of technology...? And then sub-questions like how technology affects, influences, changes, or reshaped your daily life. Then I also let other participants share their thoughts about the same question as well, thus converting a monolog into a group conversation or discussion.

As mentioned above, in my discussions, the initial set of questions were about collecting personal information from respondents, such as names, gender, age, profession, address, occupation, and contact numbers. Linnæus university's privacy and data disclaimer were used and guidelines were followed. Relevant consent forms provided by the course co-ordinator were distributed and duly signed by participants. For discussion, I chose respondents in such a manner that all age groups were represented, so I could get a comprehensive overview of security and privacy perceptions and understanding.

The next phase of the discussion was about participants' general attitude towards technology, their perception, and knowledge about the internet of things, as well as the usability, functionality, and reasons for using IoT devices.

During my focus group session, I wrote memos. These memos are very vital for constructing categories and finding relationships between these categories. Throughout the focus group session, respondents were interviewed individually and then group discussion. After each interview, I wrote a memo showing what I had learned from that interview. These memos contained information about respondents' knowledge and awareness about subject matter and some pre-existing ideas I had in mind, in relation to what had been said in the interviews. After completing memos, my next task was to compare them and find patterns/themes.

We can say from the responses to above mentioned questions that the word Internet of things is more abstract. A smart home computer, on the other hand, is seen as something more tangible, with a focus on straightforward usability.

If I compare answers to the previous and current questions, it is easy to conclude that the phenomenon of the Internet of things (IoT) is more abstract. Simultaneously, a smart home device is perceived as a more concrete and real thing with value-creation functionalities.

The researcher pushed respondents to talk about several key points in response to each question and argue about those points with other respondents. These key points were explained by different respondents. They also formed the basis for emerging themes for grounded theory.

Chapter 5

Discussion

In the following chapter, data acquired from empirical findings is structured and aligned with literature reviews and methodology chapters to give it coherency and a logical flow. Empirical findings were merged with themes discovered from grounded theory. In the end, the researcher presented his approach, findings, and contributions and related them to the literature review chapter.

The purpose of this discussion chapter was to critically examine findings in light of the discussion in the thesis' previous chapters (introduction, literature review, methodology and empirical findings) and to express what has been learned or what were the learning outcomes. The Discussion chapter explained to the readers what my findings mean.

If I compared the answers to different questions and analyzed the discussions that took place during the focus group session, it was easy to conclude that the phenomenon of the Internet of things (IoT) was more abstract. Simultaneously, a smart home device was perceived as a more concrete and real thing with value creation functionalities.

Moreover, surprisingly, the empirical analysis of interviews showed that almost all participants had more than one IoT-based smart device at home, so IoT saturation was nearly 100%.

Participants' general knowledge, understanding, and awareness about the technology, in general, was good. Young people in the age group of 30-44 years were more tech-savvy, more enthusiastic, and curious about new technologies and gadgets. They were keen on using smart home devices, and in fact, they were already using smart watches and different mobile apps to improve their health and fitness.

As expected, people between the age group of 50-60 years were less tech-savvy and wanted to use technology only when necessary for them and to bring comfort and a sense of home security in their daily lives.

Discussion from previous chapters showed that realized benefits of IoT devices included increased comfort in daily life with the use of technology, cost savings, use of virtual assistants, better fitness, and improvement in home security.

Apart from mentioning the advantages of using smart home devices, appliances, or gadgets, participants also described features they would like to see in their smart devices, such as switching the

lights on and off, playing music, controlling devices with voice commands, a kind of a single or central remote or application for all the home appliances, smart home alarms, remote home climate control systems, Wi-Fi home cameras, and robot vacuum cleaners.

Despite having a vague understanding of security and privacy issues associated with smart devices, not paying enough attention to them turned out to be one of the major drawbacks. Participants were not clear about what information was taken, how it was taken, and to what extent it was taken. They are unaware of privacy policies and purchase agreement conditions. Participants were uncomfortable with data sharing to third party companies.

56.4% of the IoT-based smart devices in the US and 83.84% of the UK are exposing personal information to third-party companies. Location data and IP addresses are the most common types of data shared by these devices with third parties (www.cyware.com). Previous research has revealed that when smart home devices such as TVs, virtual assistants, smart speakers, doorbells, and appliances were analysed, they were sending user information to third party companies, including Netflix, Spotify, Microsoft, Akamai, and Google. This argumentation confirmed the researcher's data from questions 20 to 27.

Almost all the participants raised third-party involvement when talking about smart home devices. They said we, as users and companies, should strike a balance between privacy, security, trust, and usability of the products. Then that young tech-savvy guy belonging to the 30-40 yrs. age group mentioned a reference from the social media about a cybercrime, involving smart home devices and where people's trust was breached without their knowledge.

Based on the empirical findings and their analysis, the following similarities or patterns were discovered in the collected data:

5.1 Familiarity with Smart Homes and Internet of Things

It became obvious with initial analysis that targeted respondents were well versed in the concepts of smart homes and had reasonable familiarity with IoT.

5.2 Use of technology and smart devices

Another common theme proved to be participants' awareness of technology and the use of smart devices in their homes. Every one of the ten participants uses regular to advanced-level technology in their homes, ranging from appliances to smartphones and watches.

5.3 IoT devices as an improvement in quality of life

Another recurring theme was the general agreement that technology and smart home devices play a role in bringing comfort and peace of mind to daily routines and life. Participants from all age groups mentioned that their reason for buying these devices/gadgets was to save time, money, and effort in doing different things. These include planning a trip out, automation of lighting and heating, smart locks which can be managed from a mobile device, playing favorite music, and saving some preferences in virtual assistants so they can act on them when they arrive home from work or vacation.

5.4 Ordinary security resilience

Another interesting, rather surprising common factor was knowledge and resilience towards basic security measures. Participants tend to update their router passwords regularly. Followed general password requirements (medium to strong passwords). Even middle-aged and elderly participants

update their passwords, although not very often. Participants were using "password vaults" to keep their passwords in the same and secure place and were using a master password to access their vaults.

5.5 Lack of true security and privacy understanding

Although people were updating router passwords, they were found not to be too keen on updating smart home devices and their passwords. The worrying factor was not knowing the real threat of information or data leakages, exploitation, and misuse. It was observed across all participants that their knowledge and awareness levels were average when it came to knowing to what extent they were at risk, the nature of risks, and potential consequences in case something happened.

5.6 3rd party involvement

Data collection and its unauthorized use, or even selling data without the knowledge of participants, was another important issue. Device/gadget manufacturers collect consumer data. Third-party data sources include smart home devices, websites, social media networks, surveys, and different subscriptions. This data is then sold to marketing and advertising companies for targeted marketing, personalized ads, etc. Participants generally were not aware of how much their personal information was shared with local municipalities, government bodies, local companies, and international multinational giants. It has been observed that in most cases, it was done without the permission of the participants.

5.7 Willing to buy smart home devices again?

Another common point was participants' willingness and desire to buy smart home devices again. Most of the participants were satisfied with the functionality and purpose of the devices they were bought for. Participants described them as a technology of the future and a common site in every household. They are convinced that this technology will mature and the induction of 5G will provide endless opportunities with smart home devices.

These categories and above described findings are directly connected to authentication, authorization, trust, privacy, confidentiality, 3rd party data and access control factors identified in the literature review chapter.

There are multiple solutions available to deal with them. The use of digital signatures and certificates is especially important for IoT devices. session keys and tokens can also be used to ensure authentication (Skarmeta, Ramos and Moreno, 2014). It is important to know that the majority of certificate-based and signature-based authentication systems depend on a trusted third party or certificate authority to verify that the individual is who it claims to be. Strong passwords and changing them regularly is also very vital here, as described in sections 4.1 and 4.2.

Since ordinary people are not very tech-savvy, or depending upon which age group is using IoT devices, it's difficult to apply complex IoT based solutions directly (Anggorojati, 2015). As a result, it is easy to see that people must have some basic to intermediate technical skills in order to manage logins, gain access to all information, and control functions in smart home devices. Academic researchers emphasize the capability-based approach for people using IoT devices (Gusmeroli, Piccione, and Rotondi, 2013).

Another important concern of people was data confidentiality and integrity. They were not sure which device was collecting what data and how much data. People need to read the description of their IoT product thoroughly to get a basic overview of how the device works and uses their home network and other resources. People should look at what type of encryption their device offers. The primary means

of ensuring confidentiality and integrity in smart home devices is the use of encryption and cryptographic mechanisms. are two popular methods for encrypting data: symmetric and asymmetric. Both can be used in IoT devices. Although each scheme has its own set of benefits and drawbacks (Bafandehkar, Yasin, Mahmod, and Hanap, 2013), But it was evident from the empirical findings of section 5.1, that people were only interested in ease of use and what comfort it would bring, and they were least interested in knowing about the security mechanisms behind their devices.

Since young and middle-aged people were more tech savvy, as reflected by interview data, they were and should look for devices that offer logins and entrance to devices via digital signatures and hash functions (Gallagher and Kerry, 2013) to maintain the integrity of their smart watches, smart music systems, smart virtual assistants, smart lighting and heating systems, as these were the major uses found in empirical data.'

It has been observed that even before making a purchase, people must overcome significant obstacles with regard to choosing the right product and are often overwhelmed and confused by the sheer number of available devices, making it difficult to translate their needs into the required smart device and trust them. This situation creates the issue of trust man agent.

The Internet of Things (IoT) enables smart devices to be used anywhere and at any time via the Internet. These devices must be secured via the Internet network and must trust other devices in order to interact with them, mostly through protocols that give birth to security threats. The type of IoT architecture has a significant impact on how trust is built. For instance, people in Valby were using intelligent virtual assistants (IVAs) like Alexa and Google but were not aware of which trust and privacy breaches they were facing while making calendar appointments, ordering food, turning Philips Hue on and off, listening to music, or making shopping lists. People need to learn how to build and manage trust in a smart home environment.

People's trust in a product is a major driver of its success in the majority of cases. As a result, there is a need for people to better understand and improve how smart home devices interact with one another and build trust not only among themselves but how that trust can be established with users as well (Pavlidis, 2011). People must not make any trusting assumptions.

It has been observed with empirical data analysis that all respondents were using internet routers, and all of them changed their default passwords. In fact, they were using password vaults to manage passwords, but still were not bothered or concerned about the security of the internet network, which connects their devices to the router. They were not aware of the importance of their home network and the majority of them only knew about the built-in security layer (firewalls) provided by their router. This awareness needs to be communicated among people, and it is not that difficult to implement difficult security measures for home networks.

Generally, IoT ecosystems include a large number of devices, and the ability to decide whether or not a device can be trusted over a network is critical from a security point of view (Bao et al. 2013). People can take simple measures to secure their smart home devices connected over the home network. These measures can include setting up their router correctly, changing the router's default company name, unique passwords, strong encryption, separate home network for smart home devices. Continuously update the router and smart home devices, disabling unnecessary functions.
Energy conservation is a top priority for people. But they have to realize that the ability to adapt and self-configure is a valuable trait for the Internet of Things, particularly as the number of IoT devices

being deployed and connected to the internet is constantly increasing. Most security solutions and frameworks take a static approach to security, enforcing a mechanism all of the time and not adapting to the context in which the IoT device is running. However, these methods lack versatility and the ability to decide when security can take priority over energy conservation (Hamdi and Abie, 2014).

The middle-aged and older participants were not fully utilizing the potential of their IoT devices. It was a younger group of people who were more into smart devices. This could be because sometimes the benefits of IoT devices lack clear understanding or do not reflect the true advantage of their use. Therefore, the subjective added value of smart home IoT devices remains ambiguous for certain groups of people. It is learned from literature review, interview data, and data analysis that interoperability between devices from different manufacturers creates uncertainty and necessitates trade-offs between flexibility and ease of installation. People find it considerably hard to link different IoT devices from different manufacturers, and that leads to underutilized functionality of the device.

3rd party involvement in people's personal data collection and usage proved to be an area of serious concern. People were aware, but to a limited extent, of the data collected by their smart home devices.

Middle-aged and elderly people did know how Amazon and Google were permanently collecting data from their smart home devices in the name of improving their services. This information is then sold to 3rd parties for marketing and selling purposes. This means Amazon and Google will know when users of their gadgets are at home, when they go to sleep, and even what TV channels they watch and when they watch them, all without any input from the users of their intelligent virtual assistants (IVAs) like the Echo or the Google Home. The data generated would be continuously reported, allowing marketing and consumer companies to get an idea of people's behaviours and lifestyles.

Besides having ordinary security resilience, people are not often concerned about maintaining security during the use of smart devices. Furthermore, uncertainty about the devices' future security, particularly in the context of rapid technological development, and high acquisition costs seem to be additional barriers for few of them.

The results of these findings will be shared on the official Facebook page of my residential building. I will summarise all these findings on a single A4 page, give it a more article-like shape, and publish it here: https://www.facebook.com/groups/2646909905396407

These findings will also be shared with the local community where I live in Valby, Copenhagen, on the following page: https://www.facebook.com/groups/552855045130208.

Finally, I have contacted our local community newspaper to publish my article and findings in their weekend edition so they can reach an audience, especially the elderly who are not online. That newspaper is called "Valby lokalavisen". They also have an online version, which can be seen at: https://www.e-pages.dk/lokalavisenvalby/72/.

6. Conclusion

The study aimed to provide an explicit overview of the most important aspects of the internet of things (IoT) with a particular focus on the security, integrity, and privacy threats this phenomenon poses, as well as people's understanding of these risks.

The three main research questions of the thesis were:

I. What security, privacy, and trust issues are associated with IoT devices?
II. How much do people understand and care about security, privacy, and safety in terms of IoT devices...?
III. What factors people must consider when buying and using IoT devices…?

These questions were addressed in the following way: A list of security and privacy risks has been produced after conducting a comprehensive literature review. These risks were addressed and discussed in relation with empirical data gathered from interviews during focus group session. Empirical findings and their analysis with grounded theory was conducted that helped me to become familiar with the general understanding of people in the context of security and privacy issues related to IoT devices.

Findings showed, the degree to which people were aware of the risks associated with IoT devices correlated with their age and interest in technology. The greater a person's interest in technology, the more aware he was about the threats. In the same way, young people proved to be more agile, careful, and keen on knowing about security and privacy and how to secure their devices as compared to older ones.

Despite the fact that many people were aware of the risks associated with IoT devices, they didn’t actively secure their IoT devices. The reason was lack of information about how to secure devices/gadgets. People were not aware of authentication, authorization, privacy and trust factors of security while buying and using their devices. Use of intelligent virtual assistants (IVA) has also exposed them to possible home network compromises, helped by their password setting behaviors.

Lastly, smart homes and smart home devices are here to stay. However, in an ever-expanding sea of brands, devices, ecosystems, AI platforms, it can be difficult to decide what to buy without feeling like you're missing something or making the wrong choice. To avoid this, here are my suggestions for what to look for when shopping for IoT based smart home devices:

- Make sure the IoT device you are planning to purchase is secure by design.
- If the manufacturer is unable to provide sufficient details about the device's security approach, think twice about buying that IoT device.
- Check and make sure, that the manufacturer will provide timely patches and updates for the entire life span of the device.
- Don’t connect your smart device to the internet unless required. If it can work offline, use that option and don't compromise on your privacy and security.
- Normally, a good home Wi-Fi router is capable of creating multiple networks. An extra network just for the internet of things devices can be created. Using a separate network serves as a buffer, ensuring that no outside party can access your shared files or other forms of encrypted data.

- It's very crucial to update the passwords on your internet of things devices/gadgets. Make sure each device has its own password. To remember passwords, a password manager can be used. Update passwords at least twice a year.
- UPnP is a plug-and-play feature of almost all IoT devices. Different devices use this feature to locate and connect to one another. Since we don't have to configure each device individually, this feature makes the devices more convenient. However, we should be aware that UPnP protocols depend on local networks to communicate thus making them vulnerable to outside access. Criminals can gain access to number of devices simultaneously if there is an attack. Therefore, turning off the UPnP function on your device is a good idea.
- If automatic updates are available on your device, switch them on, otherwise, search for firmware updates on a regular basis to secure your device.
- A number of IoT device manufacturers also provide cloud storage with their devices. However, before you begin using the cloud, make sure you are familiar with the ways of protecting your data and that you completely comprehend the privacy policy.
- In the case of wearable devices, when you go to a public place, it connects with the free Wi-Fi and your data becomes instantly accessible to whoever is connecting to the same network. So when you're not using your wearable gadgets, make sure they are turned off.
- Some IoT devices need to be connected to the internet at all times, in order to function properly. There can also be some devices that don’t provide as much efficiency as promised. Therefore, regularly evaluate the functionality of your devices. If they don't add much value to your daily life or to comfort or if they seem dangerous, just get rid of them. Alternatively, if there is a single device that can replace a number of others, invest in it.

6.1 Contribution

The contributions of said study are to divert people’s attention towards hidden and potentially risky factors of IoT devices and to increase the level of understanding among ordinary people about emerging technologies such as Internet of things (IoT), which they are using in different forms in their daily lives. Thesis report followed a holistic approach while explaining, what the internet of things is? What are its key components and enabling technologies? What is its architecture and how does it work? People were presented with the facts that, how crucial it is to be aware of the security and privacy risks posed by these smart devices. In the end, a list of bullet points is produced which can be used as a checklist or reference point when buying a smart home device.

6.2 Future Research

Future privacy and security research should focus on "why current solutions fail to secure security loopholes and what best practices should be followed to avoid such scenarios in the future". The researcher should and will focus on collective team efforts to battle these security and privacy challenges. This means computer scientists, data scientists, developers, project managers, and cybersecurity experts are required to pool their expertise to neutralize these threats. But a serious challenge will be, how to face and solve new and unseen security and privacy threats emerging every single day.

How IoT device manufacturers and governments perceive the phenomenon of privacy and security in the context of future smart homes can be a great research question.

Keeping in mind the results of empirical findings, further research on development of a common production and regulatory framework for IoT producers can be another relevant and important area to focus on. On the other hand, as mentioned in the discussion chapter, from the consumer's perspective, development of general data protection regulation (GDPR) to protect the general public's personal information is also a valid and relevant research and legislation area for governments.

The coming decades promise to dramatically change how we perceive digital devices and digital environments, and it is very important that we are prepared for these novel developments and advancements. Emerging threats and scenarios must be investigated and dealt with accordingly in order to anticipate security and privacy risks in the coming decade.

7. References

Abdmeziem, M.R. and Tandjaoui, D. 2014. Tailoring mikey-ticket to e-health applications in the context of internet of things. In International Conference on Advanced Networking, Distributed Systems and Applications (Short Papers), pages 72–77, June.

Abrams, L. 2018. "Dramatic Increase of DDoS Attack Sizes Attributed to IoT Devices,"

Abomhara, M. and Koien, G. 2014. Security and privacy in the Internet of Things: Current status and open issues. 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS).

Addo, I. D., Ahamed, S. I, Yau, S. S and Buduru, A. 2014. A reference architecture for improving security and privacy in internet of things applications, in Mobile Services (MS), 2014 IEEE International Conference on. IEEE, 2014, pp. 108115.

Aggarwal, R. and Das, M.L. 2012. August. RFID security in the context of internet of things. In Proceedings of the First International Conference on Security of Internet of Things (pp. 51-56).

Ahmad, I. 2018. "How The Internet of Things Could Be Putting Your Home at Risk,".

Ahmad, R., Christian W and Michael W. 2015. Security and privacy challenges in industrial Internet of Things, 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC).

Alcaide, A., Palomar, E., Montero-Castillo, J. and Ribagorda, A. 2013. Anonymous authentication for privacy-preserving IoT target-driven applications. Computers & Security, 37, pp.111-123.

Aleisa, N. and Renaud, K. 2017. Privacy of the Internet of things: a systematic literature review. In: HICSS, proceedings of the 50th Hawaii international conference.

Alaba, F., Othman, M., Hashem, I. and Alotaibi, F. 2017. Internet of Things security: A survey. Journal of Network and Computer Applications, 88, pp.10-28.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. 2015. Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), pp.2347-2376.

Alexander, R. and Tsao, T. 2012. Adapted Multimedia Internet KEYing (AMIKEY): An extension of Multimedia Internet KEYing (MIKEY) Methods for Generic LLN Environments draft-alexander-roll-mikey-lln-key-mgmt-04, (Work in Progress), IETF, Tech. Rep., September 2012.

Anggorojati, B. 2015. Access control in iot/m2m-cloud platform, _ Ph.D. dissertation, Aalborg University.

Arabo, A. and Pranggono, B. 2013, May. Mobile malware and smart device security: Trends, challenges and solutions. In 2013 19th International Conference on Control Systems and Computer Science.

Ashraf, Q. M. and Habaebi, M. H. 2015. Autonomic schemes for threat mitigation in internet of things, _ Journal of Network and Computer Applications, vol. 49, no. 0, pp. 112 _ 127, 2015.

Atzori, L., Iera, A. and Morabito, G. 2014. From" smart objects" to" social objects": The next evolutionary step of the internet of things. IEEE Communications Magazine, 52(1), pp.97-105.

Bao, F., Chen, I. R., and Guo, J. 2013. Scalable, adaptive and survivable trust management for community of interest-based internet of things systems, in Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh In- ternational Symposium on, March 2013, pp. 17.

Bafandehkar, M., Yasin, Md., Mahmod R., and Hanapi, Z. M. 2013. Comparison of ecc and rsa algorithm in resource constrained devices, in IT Convergence and Security (ICITCS).

Benabdessalem, R., Hamdi, M., and Kim, T. H. 2014. A survey on security models, techniques, and tools for the internet of things, _ in Advanced Software Engineering and Its Applications (ASEA), 2014 7th International Confereence on. IEEE, 2014, pp. 44_48.

Bhattacherjee, A. 2012. Social science research: Principles, methods, and practices.

Borgohain, T., Kumar, U. And Sanyal, S. 2015. Survey of security and privacy issues of internet of things, Xiv:1501.02211.

Borgohain, T., Kumar, U., and Sanyal, S. 2015. Survey of security and privacy issues of internet of things, _ arXiv preprint arXiv:1501. 02211.

Braun, V and Clarke, V. 2006. Using thematic analysis in psychology. Qualitative Research in Psychology, 3, 77–101.

Burgess, R.G. 1984. In the Field: An Introduction to Field Research. London: Unwin Hyman.

Burg, A., Chattopadhyay, A. and Lam, K., 2018. Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things. Proceedings of the IEEE, 106(1), pp.38-60.

Byres, E. and Lowe, J. 2004. "The myths and facts behind cyber security risks for industrial control systems", Technical report PA Consulting Group, 2004.

Chan, M., Campo, E., Estève, D. and Fourniols, J.Y. 2009. Smart homes—current features and future perspectives. Maturitas, 64(2), pp.90-97.

Cerullo, Gianfranco & Mazzeo, Giovanni & Papale, Gaetano & Ragucci, Bruno & Sgaglione, Luigi. (2018). IoT and Sensor Networks Security.

Cherkaoui, A., Bossuet, L., Seitz, L., Selander, G., and Borgaonkar, R. 2014. New paradigms for access control in constrained environments, in Recon_g- urable and Communication-Centric Systems-On-Chip (ReCoSoC), 2014 9th International Symposium on. IEEE, 2014, pp. 1_4.

Cisco.com. Available at: < https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html> [Accessed 10 Sep 2021].

Cisco.com. Available at: <https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html> [Accessed 01 Sep 2021].

Cook, D. J. and Das, S. K. 2007. "How smart are our environments? An updated look at the state of the art", Pervasive Mob. Comput., vol. 3, no. 2.

Costin, A., Zaddach J., Francillon A. and Balzarotti, D. 2014. "A large-scale analysis of the security of embedded firmwares", USENIX Conference on Security Symposium.

Creswell, J. W. 2017. Research Design – Qualitative, Quantitative and Mixed Methods Approaches (4th ed). [e-book] London: SAGE, 273 pages.

Cui, A. and Stolfo, S. J. 2010. "A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan", Annual Computer Security Applications Conference (ACSAC).

Cyware.com. Available at: <news/iot-devices-send-user-data-to-third-parties-including-netflix-microsoft-and-google-b2724821> [Accessed 15 aug 2021].

Das, M. L. 2015. Privacy and security challenges in internet of things, in Distributed Computing and Internet Technology. Springer, 2015, pp. 3348.

David, Aaker, A., Kumar, V., Day, George S. 2000. Marketing Research [e-book] 7th Ed. John Wiley & Sons.

Denzin, N.K. 1989. The sociological interview. In The Research Act: A Theoretical Introduction to Sociological Methods. New Jersey: Prentice Hall, 102-120.

De Saint-Exupery, A. 2009. “Internet of things, strategic research roadmap,”.

De Villiers, M.R. 2005. ”Three approaches as pillars for interpretive information systems research: development research, action research and grounded theory.” In Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries (pp. 142-151).

Denscombe, M. 2014. The good research guide: for small-scale social research projects. McGraw-Hill Education (UK).

Du, L., Guo, J. and Li, Y. 2013. Research on micro-certicate based authentication protocol, in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering. Atlantis Press, 2013.

Dzung, D., Naedele, M., von Hoff, T. and Crevatin, M. 2005. "Security for industrial communication systems", Proceedings of the IEEE, vol. 93, no. 6.

Easterby M., Thorpe, R., and Lowe, A. (2002): ”Management Research: An Introduction” (2nd ed.) London, UK: SAGE.

Erguler. 2014. A potential weakness in r_d-based internet-of-things systems, _ Pervasive and Mobile Computing, no.

Evans, D., 2012. [online] Cisco.com. Available at: <https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf> [Accessed 21 May 2020].

Finlay, D. 2016. Smart Bandage Technologies-Design and Application. 978-0-12-803762-1, Copyright © 2016 Elsevier Inc. All rights reserved.

Flannigan, J. 2016. “Parental Warnings: baby Monitors Can Be Hacked,” 18 August.

Fontana, A., and Frey, J.H. 2005. The interview: From neutral stance to political involvement.

Forsberg, D., Ohbay, B. Patil, H. and Yegin, A. 2008. Protocol for Carrying Authentication for Network Access (PANA), Internet Requests for Comments, IETF, RFC 5191, May 2008.

Franz, C.R. and Robey., D. 1984. "An Investigation of User-Led System Design: Rational and Political Perspectives," Communications of the ACM, Volume 27, Number 12, December 1984, pp. 1202-1217.

Frankel, S. and Krishnan, S. 2011. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, Internet Requests for Comments, IETF, RFC 6071, Feb 2011.

Gartner. 2014. Available at: <https://blogs.gartner.com/svetlana-sicular/the-era-of-data/> [Accessed 21 May 2021].

Gallagher, P. and Kerry, C. 2013. Fips pub 186-4: Digital signature standard, dss.

Glover, B. and Bhatt, H. 2006. RFID essentials. " O'Reilly Media, Inc.".

Glaser, B. 1992. Basics of grounded theory analysis: Emergence vs. forcing. Mill Valley, CA: Sociology Press.

Greengard, S. 2015. The Internet of Things, [e-book] MIT press, ISBN: 978-0-262-52773-6.

Groves, Robert, M., Fowler, Floyd, J., Couper, Mick, P., Lepkowski, James, M., Singer, Eleanor and Tourangeau. 2004. Survey methodology. Hoboken, NJ: John Wiley & Sons.

Grossoehme, DH. 2014. Overview of qualitative research. J Health Care Chaplain. 2014; 20:109–22.

Gregor, S. 2006. The Nature of Theory in Information Systems. MIS Quarterly, 30(3), pp. 611-642.

Grossklags, J. and Good, N. 2007. Empirical studies on software notices to inform policy makers and usability designers, _ in Financial Cryptography and Data Security. Springer, pp. 341_355.

Granjal, J., Monteiro, E., and Silva, J. 2015. Security for the internet of things: A survey of existing protocols and open research issues, _ Communications Surveys Tutorials, IEEE, vol. PP, no. 99.

Gubbi, J. Buyya, R. Marusic, S. Palaniswami, M. 2013. Internet of Things (IoT): A vision, architectural elements, and future direction. Future Generation Computer Systems, 29(7 Sept. 2013), pp. 1645-60.

Gusmeroli, S., Piccione, S. and Rotondi, D. 2013. A capability-based security approach to manage access control in the internet of things, Mathematical and Computer Modelling, vol. 58, no. 56, pp. 1189 1205, 2013, the Measurement of Undesirable Outputs: Models Development and Empirical Analyses and Advances in mobile, ubiquitous and cognitive computing.

Guoqiang, H., Wee Peng, T., and Yonggang, W. 2012. Cloud robotics: Architecture, challenges and applications. IEEE Network, June.

Guba, Egon, G., Lincoln, and Yvonna, S. 1998. Competing paradigms in qualitative research. In Norman K. Denzin & Yvonna S. Lincoln (Eds.), The landscape of qualitative research (pp.195-220). Thousand Oaks, CA: Sage.

Hamdi, M. and Abie, H. 2014. Game-based adaptive security in the internet of things for ehealth, _ in Communications (ICC), 2014 IEEE International Conference on. IEEE, 2014, pp. 920_925.

Harling, K. 2002. An Overview of Case Study. Agricultural Economics, 4, 1-7.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B., 2019. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access, 7, pp.82721-82743.

Harrie and Jansen. 2010. The Logic of Qualitative Survey Research and its Position in the Field of Social Research Methods [63 paragraphs]. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 11(2), Art. 11.

Hernandez, G., Arias, O., Buentello, D. and Jin, Y. 2014. "Smart Nest thermostat - A smart spy in your home", BlackHat USA.

Hernandez, J. Ramos, M. Pawlowski, A. Jara, A. Skarmeta Gomez, and Ladid, L. 2015. _Towards a lightweight authentication and authorization framework for smart objects, _ Selected Areas in Communications, IEEE Journal on, vol. PP, no. 99, pp. 1_1.

Hussen, H., Tizazu, G., Ting, M., Lee, T., Choi, Y. and Kim, K.H. 2013. Sakes: Secure authentication and key establishment scheme for m2m communication in the ip-based wireless sensor network (6l0wpan), in Ubiquitous and Future Networks (ICUFN), 2013.

Iacobucci, Dawn, Gilbert, A., Churchill, Jr. 2018. Marketing Research: Methodological Foundations 12 th ed. [e-book] CreateSpace Independent Publishing Platform.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., and Qiu, D. 2014. Security of the internet of things: perspectives and challenges, _ Wireless Networks, vol. 20, no. 8, pp. 2481_2501, 2014.

Joseph, R. 2018. “My Friend Cayla: the doll for children accused of 'illegal espionage',”.

Kasper, T., Oswald, D., and Paar, C. 2014. Sweet dreams and nightmares: Security in the internet of things, in Information Security Theory and Prac- tice. Securing the Internet of Things. Springer, pp. 1_9.

Kagermann, H., Wahlster, W. and Helbig, J. 2013. Securing the future of German manufacturing industry - Recommendations for implementing the strategic initiative Industrie 4.0, 2013.

Kanuparthi, A., Karri, R. and Addepalli, S. 2013. Hardware and embedded security in the context of internet of things, in Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles. ACM, 2013, pp. 6164.

Kagermann, H., Wahlster, W. and Helbig, J. 2013. Securing the future of German manufacturing industry Recommendations for implementing the strategic initiative Industrie 4.0.

Keoh, S. L., Kumar, S. and Tschofenig, H. 2014. Securing the internet of things: A standardization perspective, _ Internet of Things Journal, IEEE, vol. 1, no. 3, pp. 265_275, June.

Khoo, B. 2011. enabler of the internet of things: issues of security and privacy, _ in Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing. IEEE, pp. 709_712.

Koushanfar, F., Sadeghi, A.R. and Seudie, H. 2012. "Eda for secure and dependable cybercars: Challenges and opportunities", Proceedings of the 49th Annual Design Automation Conference.

Koscher, K., Czeskis, A., Roesner, F., S., Patel, T., Kohno, S. and Checkoway, et al. 2010. "Experimental security analysis of a modern automobile", IEEE Symposium on Security and Privacy (S&P), 2010.

Kumar, J. S. and Patel, D. R. 2014. "A survey on internet of things: Security and privacy issues", International Journal of Computer Applications, vol. 90, no. 11.

Kvale, S. 2006. Dominance through interviews and dialogues. Qualitative inquiry, 12(3), pp.480-500.

Lee and Liebenau. 1997. Information Systems and Qualitative Research. © Springer Science+Business Media Dordrecht 1997.

Lee, S., Bae, M. and Kim, H. 2017. Future of IoT Networks: A Survey. Applied Sciences, 7(10), p.1072.

Liu, C., Zhang, Y., Cai, Z., Yang, J. and Peng, L. 2013. Artificial immunity-based security response model for the internet of things, _ Journal of Computers, vol. 8, no. 12, pp. 3111_3118.

Li, S., Tryfonas, T. and Li, H. 2016. The Internet of Things: a security point of view. Internet Research, 26(2), pp.337-359.

Liu, Y. and Zhou, G. 2012. "Key technologies and applications of internet of things", 5th International Conference on Intelligent Computation Technology and Automation (ICICTA).

Luo, M., Tu, M. and Xu, J. 2014. A security communication model based on certi_cateless online/o_ine signcryption for internet of things, _ Security and Communication Networks, vol. 7, no. 10, pp. 1560_1569.

Mashal, I., Alsaryrah, O., Chung, T.Y., Yang, C.Z., Kuo, W.H. and Agrawal, D. P. 2015. “Choices for interaction with things on Internet and underlying issues,” Ad Hoc Networks, vol. 28.

Mattord, H. And Whitman, M. 2018. Management of Information Security, 6th Edition, Cengage Learning, ISBN: 9781337405713.

Mark, S., Philip, L. and Adrian, T. 2000. Research Methods for Business Students (5th ed), [e-book] Pearson Education.

McKinsey Global Institute. 2021. https://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact.

Medaglia, C. and Serbanati, A. 2010. "An overview of privacy and security issues in the internet of things" in The Internet of Things, Springer.

Mendez, Papapanagiotou and Yang. 2017. Internet of Things: Survey on Security and Privacy. Information Security Journal a Global Perspective · July 2017.

Medaglia, C. and Serbanati, A. 2010. "An overview of privacy and security issues in the internet of things" in The Internet of Things, Springer.

Miller, B. and Rowe, D. 2012. "A survey SCADA of and critical infrastructure incidents" in Research in Information Technology (RIIT), ACM, 2012.

Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamta, I. 2012. Internet of things: Vision, applications and research challenges. Ad Hoc Networks, pages 1497–1516, April 2012.

Minichiello, V., Aroni, R., Timewell, E. and Alexander, L. 1990. In-depth Interviewing: Researching people. Hong Kong: Longman Cheshire Pty Limited.

Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. 2012. "Survey internet of things: Vision applications and research challenges", Ad Hoc Netw., vol. 10, no. 7.

Mikko, L. and Hypponen, N. 2014. “The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation,” Technology Innovation Management Review.

Modadugu, N. and Rescorla, E. 2012. Datagram Transport Layer Security Version 1.2, Internet Requests for Comments, IETF, RFC 6347, January 2012.

Moskowitz, R. and Hummen, R. 2014. HIP Diet EXchange (DEX) draft-moskowitz-hip-dex-02, (Work In Progress), IETF, Tech. Rep., December 2014.

Ndibanje, B., Lee, H.J., and Lee, S.G. 2014. Security analysis and improvements of authentication and access control in the internet of things, _ Sen- sors, vol. 14, no. 8, pp. 14 786_14 805.

Oh, D., Kim, D., and Ro, W,. 2014. A malicious pattern detection engine for embedded security systems in the internet of things, Sensors, vol. 14, no. 12, pp. 24 18824 211, 2014.

Pallavi, S., Smruti, R. and Sarangi. 2017. Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, Volume 2017, Article ID 9324035.

Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L. and Chen, H. 2014. Uninvited connections: A study of vulnerable devices on the internet of things (iot), _ in Intelligence and Security Informatics Conference (JISIC), IEEE Joint. IEEE, 2014, pp. 232_235.

Pavlidis, M. 2011. Designing for trust. In: CAiSE (Doctoral Consortium). pp. 3–14.

Perera, C., Ranjan, R., Wang, L., Khan, S.U. and Zomaya, A.Y. 2015. Big data privacy in the internet of things era. IT Professional, 17(3), pp.32-39.

Post-gazette.com. Available at: <business/tech-news/2019/11/14/University-of-Michigan-researchers-use-laser-to-hack-voice-activated-devices-like-Amazon-Echo/stories/201911140069> [Accessed 18 Aug 2021].

Priya, I., Pathak., and Tripathi, A. 2018. "Big Data, Cloud and IoT: An Assimilation," Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T), 2018, pp. 34-40.

Punch, K.F. 1998. Introduction to Social Research: Quantitative and Qualitative Approaches. Thousand Oaks: Sage.

Raza, S., Wallgren, L., and Voigt, T. 2013. Svelte: Real-time intrusion detection in the internet of things, Ad hoc networks, vol. 11, no. 8, pp. 2661_2674, 2013.

Rekleitis, E., Rizomiliotis, P. and Gritzalis, S. 2011. How to protect security and privacy in the iot: a policy-based rd tag management protocol, Security and Communication Networks, 2011.

Rghioui, A., L'aarje, A., Elouaai, F. and Bouhorma, M .2014. The internet of things for healthcare monitoring: Security review and proposed solution, in Information Science and Technology (CIST), 2014 Third IEEE Inter- National Colloquium in, Oct 2014, pp. 384389.

Riggins, F.J. and Wamba, S.F. 2015. January. Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics. In System Sciences (HICSS), 2015 48th Hawaii International Conference on (pp. 1531-1540). IEEE.

Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z. and Bouabdallah, A. 2013. A systemic approach for IoT security. In 2013 IEEE international conference on distributed computing in sensor systems (pp. 351-355). IEEE.

Roman, R., Najera, P. and Lopez, J. 2011. Securing the internet of things, Computer, vol. 44, no. 9, pp. 51_58, 2011.

Rodgers, B.L., Cowles, K.V. 1993. The qualitative research audit trail: A complex collection of documentation. Res Nurs Health. 1993; 16:219–26.

Rowley, J. 2002. Using Case Studies in Research. Management Research News, 25, 16-27.

Robertson, M.H.B. and Boyle, J.S. 1984. Ethnography: Contributions to nursing research. Journal of Advanced Nursing, 9, 43-49.

Rostami, M., Koushanfar, F. and Karri, R. 2014. "A primer on hardware security: Models methods and metrics", Proceedings of the IEEE 2014.

Saunders, M., Lewis, P. and Thornhill, A. 2009. Research Methods for Business Students. Pearson, New York.

Schurgers, Curt. and Srivastava, M.B. 2001. Energy efficient routing in wireless sensor networks. IEEE Military Communications Conference MILCOM. Communications for Network-Centric Operations: Creating the Information Force, 1:357–361, 2001.

Seitz, L., Goran, S. and Christian, G. 2013. Authorization Framework for the Internet-of-Things. ∗Security Lab, SICS Swedish ICT, Sweden †Security Research, Ericsson Research, Sweden.

Shin, D. 2014. A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things. Telematics and Informatics, 31(4), pp.519-531.

Shahrjerdi, D., Rajendran, J., Garg, S., Koushanfar, F. and Karri, R. 2014. "Shielding and securing integrated circuits with sensors", Computer-Aided Design (ICCAD) 2014 IEEE/ACM International Conference on.

Shi, W., Kumar, N. P., Gong, Chilamkurti, N. and Chang, H. 2014. On the security of a certi_cateless online/o_ine signcryption for internet of things, _ Peer-to-Peer Networking and Applications, pp. 1_5.

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D. and Coen-Porisini, A. 2014. A security-and quality-aware system architecture for internet of things, _ Information Systems Frontiers, pp. 1_13.

Silverman, D. 2009. Doing Qualitative Research; p. 472. 3rd ed. Newbury Park, London: SAGE Publications Ltd; 2009.

Skarmeta, A., Hernandez-Ramos, J. and Moreno, M. 2014. A decentralized approach for security and privacy challenges in the internet of things, _ in Internet of Things (WF-IoT), 2014 IEEE World Forum on, March 2014, pp. 67_72.

Skarmeta and Moreno, M. 2014. Internet of things, _ in Secure Data Management, ser. Lecture Notes in Computer Science, W. Jonker and M. Petkovi¢, Eds. Springer International Publishing. pp. 48_53.

Soullie, A. 2014. "Industrial control systems: Pentesting PLCs 101", BlackHat Europe.

Stojkoska, B.L.R. and Trivodaliev, K.V. 2017. A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140, pp.1454-1464.

Strauss, A. 1991. A personal history of the development of grounded theory. Qualitative Family Research5(2) (1991).1–2.

Stojmenovic, I., Jeong, H. Y. and Yi, G. 2015. Springer Berlin Heidelberg. 2015. vol. 330, pp. 691_696.

Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G. and Suciu, V. 2013. Smart cities built on resilient cloud computing and secure internet of things. In: IEEE, 19th international conference on control systems and computer science. Bucharest, Romania, 29-31 May 2013. New York: IEEE.

Suo, H., Wan, J., Zou, C. and Liu, J. 2012. Security in the internet of things: a review, _ in Computer Science and Electronics Engineering (ICCSEE), International Conference on, vol. 3. IEEE, 2012, pp. 648_651.

Vashi, S., Ram, J., Modi, J., Verma, S. and Prakash, C., 2017. Internet of Things (IoT): A vision, architectural elements, and security issues. 2017 International Conference on ISMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC).

Vermesan, O. and Friess, P. 2013. Internet of things: converging technologies for smart environments and integrated ecosystems. Aalborg: River Publishers.

Vidal Meca, F., Ziegeldorf, J. H., Sanchez, Morchon, P. M., O. G., Kumar, S. S. and Keoh, S. L. 2013. Hip security architecture for the ip-based internet of things, in Advanced Information Networking and Applications Work- shops (WAINA), 2013 27th International Conference on. IEEE, 2013.

Vucinic, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L. and Guizzetti, R. 2014. Oscar: Object security architecture for the internet of things, Ad Hoc Networks.

Wang, H., et al. 2015. Special issue on Security, Privacy and Trust in network-based Big Data. Inf. Sci. Int. J. 318(C), 48–50.

Want, R., Schilit, B.N. and Jenson, S. 2015. Enabling the internet of things. Computer, 48(1), pp.28-35.

Wedawatta, G., Ingirige, B. and Amaratunga, D. 2011. Case Study as a Research Strategy: Inves-tigating Extreme Weather Resilience of Construction SMEs in the UK. 7th Annual International Conference of International Institute for Infrastructure, Kandalama, July 2011, 1-9.

Whyte, W.F. 1960. Interviewing in field research. In Adamsn, R.N., & Preiss, J.J. (eds.), Human Organization Research. Homewood, IL: Dorsey Press, 352-374.

Whitmore, A., Agarwal, A. and Da Xu, L. 2014. The internet of things, a survey of topics and trends, _ Information Systems Frontiers, pp. 1_14.

Wilson, C., Hargreaves, T. and Hauxwell-Baldwin, R., 2015. Smart homes and their users: a systematic analysis and key challenges. Personal and Ubiquitous Computing, 19(2), pp.463-476.

Wu, M., Lu, T.J., Ling, F.Y., Sun, J. and Du, H.Y. 2010. "Research on the architecture of internet of things," (ICACTE '10), vol. 5, pp. V5-484–V5-487, IEEE, Chengdu, China.

Xu, T., Wendt, J. B. and Potkonjak, M. 2014. Security of iot systems: Design challenges and opportunities. Piscataway, NJ, USA: IEEE Press, 2014, pp. 417423.

Yao, X., Chen Z. and Tian, Y. 2014. A lightweight attribute-based encryption scheme for the internet of things, Future Generation Computer Systems.

Yin, R. K. 1994. Case Study Research Design and Methods: Applied Social Research and Methods Series. Second edn. Thousand Oaks, CA: Sage Publications Inc.

Yoon, S., Park, H. and Yoo, H. 2015. Security issues on smarthome in iot environment, _ in Computer Science and its Applications, ser. Lecture Notes in Electrical Engineering, J. J. J. H. Park, I. Stojmenovic, H. Y. Jeong, and G. Yi, Eds. Springer Berlin Heidelberg, vol. 330, pp. 691_696.

Zhu, W., Yu, J. and Wang, T. 2012. A security and privacy model for mobile r_d systems in the internet of things, _ in Communication Technology (ICCT), 2012 IEEE 14th International Conference on. IEEE, pp. 726_732.

Zhang, H. 2014. A peer to peer security protocol for the internet of things: Secure communication for the sensible things platform.

Zhao, K. and Ge, L. 2013. "A survey on the internet of things security", Computational Intelligence and Security (CIS) 2013.

Zonouz, S., Rrushi, J. and McLaughlin, S. 2014. "Detecting industrial control malware using automated PLC code analytics", IEEE Security and Privacy, vol. 12, no. 6.

Zuehlke, D. 2010. "Smart factory - towards a factory of things", Annual Reviews in Control, vol. 34, no. 1.

8. Appendixes

Appendix 1

Questionnaire for Data collection

Section 1 - Information About Respondents

1. what is your Age?
2. what is your Gender?

Section 2 – General information about technology, smart homes and IOT.

3. How much interested are you in technology?
4. Have you ever heard about Smart homes and smart devices/gadgets?
5. if yes, what comes into your mind ...?
6. How many IoT devices do you have at home...?
7. Do you have Alexa, Siri, Google Assistant or other virtual assistants at home...?
8. What services or functions, you use from your IoT devices...?
9. Do you have a router at home...?
10. Do you update your router setting regularly...?
11. Questions about router Passwords...?
12. Have you changed the password of your iot devices/gadgets in past 6 months...?
13. Do you use the same password for all devices and gadgets...?
14. Why have you purchased smart devices...?

Section 3 – Security & privacy of IoT home appliances and devices

15. How much marketing & advertising Effected your decision...?
16. How difficult or complicated these devices are to use ...?
17. Are you aware about the risks associated with IoT devices...?

18. Do you know IoT devices collect info about you ...?

19. Do you know, your iot devices can record your daily routine, likes/dislikes, choices etc...?

20. Do you know, your iot devices can spy on you...?

21. What information can go in wrong hands...?

22. Have you ever been hacked, accidently downloaded malware or installed new software without consent...?

23. Did you read the purchase agreement or privacy policy when buying these devices...?

24. Are you willing to provide more personal data if you are offered things in return e.g. special deals, discounts etc...?

25. Do you timely update, versions of your devices when prompted...?

26. What device/ gadget manufacturers should do to make them more secure...?

27. Are you satisfied with the products offered by manufacturers...?

28. based on your experiance so far , would you like to guy a smart device again ...?

Thank you for your patience, contribution and co-operation for completing this interview / focus group session.
BR
Nabeel Ahmad

Appendix 2

How to do initial coding from collected data based on comparisons

Raw data	Initial coding	Focused coding	Theoretical coding
Q. what is your general attitude towards technology.? We use different smart devices. We have advance home appliances. We know about smart homes. Q. What factors you take into account when you decided to buy this new technology.? we looked at comfort, energy savings, monetary savings and improved quality of life. we compared a few different types, talked to our social circle that had them. Marketing and advertising also influenced us. Q. Do you know these smart devices can spy on you.? We do know that these devices collect information but we had no idea, what information is collected, whom it is sold to or given to and how they use it. Q. What factors are important for you while buying smart devices.? We believe comfort, ease of use, cost, good customer support, security to some extent and availability are most important ones. Q. what manufacturers should do to produce more secure devices.? First of all, they should provide us a good customer service about product, they should clearly mention in product description that what sort of security measures we should take. There must be version updates. And products must be easy to use not to complicated screens and buttons. Q. based on your experience, will you buy smart devices again. Yes.	Young respondents more tech savvy than older. Generally, sound understanding of technology. Familiarity with concepts of smart homes and smart devices. All respondents are connected to internet and have routers. They do update passwords.	Focus must be on similarities and differences in answers. <u>Similarities:</u> interest in technology, internet and routers. Know about smart devices. Know about security and privacy risks. More awareness about privacy and security threats <u>Differences:</u> Young people more tech savvy than old aged respondents. Young one use smart devices for health improvements, listening to music and controlling smart lighting. Old people more into cost and energy savings. Less awareness about privacy and security threats. **Comparing of these codes to reach a conclusion.**	**Extract meaning out of these coding and develop novel knowledge.**

Appendix 3

How different phases of grounded theory are executed

COMPONENT	STAGE	DESCRIPTION
Openness	Entire study	Inductive analysis – preformed to construct themes out of interviews
Start Analysing	Data collection and Analysis	I started my data analysis in parallel with data collection during focus group session, to allow theoretical sampling.
Coding and comparing	Analysis	Here I broke down data into much smaller components and labelled those components. Than start comparing codes with codes and data with data, to understand and explain similarities / differences in the data. Codes were combined and related to each other in the end to transformed them into categories.
Memo writing	Analysis	I wrote the memos for every individual respondent during focus group session. The aim was to record every major detail including cross talks and comparisons.
Theoratical sampling	data collection and Sampling	My theoretical sampling consisted of coding, comparisons and memo-writing. It formed the basis of my evolving theory in the form of core themes described above. Furthermore, at this point, I tried to fill the gaps in data, removed uncertainties and kept on comparing the data obtained from respondents.
Theoratical saturation	Sampling, data collection and analysis	When my 10 respondents started repeating words or started losing interest in session, I knew study had reached its saturation point. So I stopped to maintain un-biasness.
Production of a substantive theory or Themes	Analysis and interpretation	Results are expressed as a substantive theory i.e. collection of themes that are related to one another in a logical way. For instance, In my case emerging themes were “Use of technology and smart devices, IoT devices as an improvement in quality of life, Ordinary security resilience, Lack of true security and privacy awareness, 3rd party involvement.”

Appendix 4

Consent form for taking part in Thesis:

Internet of Things
Tapping into Security and Privacy issues associated with Internet of Things

[The goal of this thesis was to better understand the phenomenon of the Internet of Things and more importantly, what security, privacy, and trust threats are associated with it. And how these threats can be overcome. Moreover, how IoT devices are perceived in terms of privacy and security by people and what factors they must keep in mind while buying, using, and disposing of such devices.]

By signing this consent form, you approve that your personal data is processed within the frame of the thesis/study described above. You can withdraw your consent at any time by contacting one of the contact persons below. In that case, your personal data will not be saved or processed any longer without other lawful basis.
The personal data that will be collected from you is [describe what personal data will be collected]. Your personal data will be processed [state period of time] and after this the data will be [deleted/archived].
You always have the right to request information about what has been registered about you and to comment on the processing of the data that has been collected by contacting one of the contact persons below or the higher education institution's personal data ombudsman on dataskyddsombud@lnu.se. Complaints that cannot be solved in dialogue with Linnaeus University can be sent to the Swedish Authority for Privacy Protection.

…… ……
Signature City and date

……
Name in block letters

Contact information:

Student's name: Nabeel Ahmad
Student's email address: na222rr@student.lnu.se

Supervisor's name: Prof David Randall
Supervisor's email address: daverandall2008@gmail.com

Linnæus University
Sweden

Faculty of Technology
SE-391 82 Kalmar | SE-351 95 Växjö
Phone +46 (0)772-28 80 00
teknik@lnu.se
Lnu.se/fakulteten-for-teknik