Faculty of Technology and Society

Department of Computer Science and Media Technology

Master Thesis Project 15p, Spring 2018

Towards Designing Open Secure IoT System

Insights for practitioners

By

Rimpu Varshney

Supervisors:

Bahtijar Vogel

Joseph Bugeja

Examiner:

Johan Holmgren

Contact information

Author:

Rimpu Varshney

E-mail: Rimpu.Varshney@gmail.com

Supervisors:

Bahtijar Vogel

E-mail: Bahtijar.Vogel@mau.se

Malmö University, Department of Computer Science and Media Technology.

Joseph Bugeja

E-mail: joseph.bugeja@mau.se

Malmö University, Department of Computer Science and Media Technology.

Examiner:

Johan Holmgren

E-mail: johan.holmgren@mau.se

Malmö University, Department of Computer Science and Media Technology.

To my inspirational father and loving mother

Abstract

IoT industry is growing at a rapid pace since everyone wants to connect everything to internet in order to use various services and applications using shared data. Openness is observed as an emerging trend in IoT industry. Security & privacy of the data are very important aspects in the design and deployment of the connected devices or Internet of Things. Fast growth in number of connected devices, heterogeneity, constrained resources, privacy, software upgrades and operational environment create important security related challenges in this domain. It is difficult to address challenges even with the considerable amount of existing work that has been done for decades in the area of security & privacy. In this research, a semi-systematic literature survey of the state of the art is conducted related to security & privacy aspects within the IoT area. The results were validated by conducting qualitative survey with IoT practitioners. The efforts have resulted towards identifying several security trends & challenges and security design aspects that can be considered by IoT practitioners in order to design an open and secure IoT system.

It can be concluded from the study that security is not only needed but is a mandatory characteristic for IoT. However, there are no general guidelines that can be proposed to address security issues since security is not only a technical problem but is more of an awareness, mindset, people and process issue. In this thesis, a novel model is proposed with openness and security characteristics. This model is grounded based on the theoretical findings and empirical data obtained from IoT practitioners. Each of the characteristics has its own design aspects that needs to be considered by IoT practitioners to design a more secure IoT system.

Keywords: IoT, Security, Privacy, Openness, Trust, Threats, Vulnerabilities, Software, Architecture, Constraints, Design.

Popular science summary

Security is finally baked into your favorite thing by trained professionals!!!

In the era, where all the devices or things are getting connected to internet at a rapid pace, we call it, “Internet of Things or IoT”. IoT is speculated to be around 18 billion devices by 2022. We are using IoT on every aspect of our life including smart homes, offices, wearables, self-driving cars, hospitals, human implants and what not. In this race, the designers of the IoT system are not giving enough consideration to the most important aspect of IoT which is security and privacy. Security of a system is not just about the technical issues but it is more related to the security awareness among the practitioners, security mindset of people and organization and processes involved, etc.

This thesis work presents an insight to the IoT practitioners with the latest security trends & challenges and provides them with security and openness aspects in order to design an open and secure IoT system. This work will benefit IoT researchers in order to analyze open and secure IoT systems from security perspective and also for IoT practitioners to implement an open and secure IoT system. Moreover, at the end it will benefit the end consumers of IoT products. Consumers could finally buy their favorite IoT thing which is developed using secure tools and processes. The thing that is secure and preserves privacy.

Acknowledgement

With great pleasure, I would like to thank all those without whom this thesis work was not possible to complete.

First of all, I am grateful to my supervisor Bahtijar Vogel for his complaisant and generous supervision throughout the study. He guided me wisely, encouraged me and supported me throughout the thesis work. I am thankful to my additional supervisor Jospeh Bugeja for his expert feedback and supervision. I extend my thanks to all the interview respondents for their valuable time, input and interest in research topic. I am also thankful to my peer reviewers for their constructive feedback.

I am especially thankful to my managers Björn Ahlberg and Nenad Pavlovic for providing me with opportunity and supporting me to complete my studies alongside my job. Special thanks to my friend Annwesh Mukherjee in supporting me throughout the study and reviewing my thesis report and providing valuable feedback.

I would also like to thank my mother, brother, family and friends. They were always supporting me and encouraging me with their best wishes.

Last but not the least without whom I wouldn't have even thought about doing my master program in computer science, my beloved wife Namita. You were always there when I needed you. You are my inspiration. Thanks for cheering me up and standing beside me.

Satakshi and Advait, thanks for always filling my life with joy and laughter and making this journey seem pretty simple. Love you my cute little kids.

Thank You All!

Hare Krishna ☺

Table of contents

List of Figures

List of Tables

List of acronyms

ACL	Access Control List
API	Application Program Interface
B2B	Business to Business
CPU	Central Processing Unit
DOS	Denial of Service
DDOS	Distributed Denial of Service
GDPR	General Data Protection Regulation
GPS	Global positioning system
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol Version 6
MMU	Memory Management Unit
NFC	Near Field Communication
OS	Operating System
PII	Person Identification Information
RAM	Random Access Memory
RFID	Radio Frequency Identification
RPL	Routing Protocol for Low Power
SOA	Service Oriented Architecture
SW	Software
UDP	User Datagram Protocol
Wi-Fi	IEEE 802.11x trademark
WSN	Wireless Sensor Network
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks

1 Introduction

This chapter introduces us to the concepts of IoT and importance of security & privacy in context of IoT. It provides motivation for conducting the study. It also discusses the problem area and defines goal and research questions to be used for this study. This chapter ends with describing the overall structure or overview of the thesis report.

1.1 IoT Introduction

In the era of connected devices popularly known as Internet of Things, humans are using services provided by IoT objects, things or devices in every aspect of their lives, including home, offices, cars, hospitals, even human bodies and others. With advent of cloud and wide deployment of Wi-Fi networks and IPv6 [29][25]. IoT is growing at an extremely fast pace. According to the mobility report published by Ericsson [1], number of IoT devices will be increased astonishingly to around 18 billion by 2022. IoT is about connecting *anything* with *anyone* at *anytime* and *anywhere* [32][35]. According to Petersen et al. [6], IoT connected devices are usually running on low power and are severely constrained when it comes to memory, processing power, battery power, space, etc. These constrained devices are usually based on micro-controllers featuring limited set of functionalities [41].

IoT is an unregulated domain and there are no standards yet agreed. As highlighted by Vogel et al. [4] and Petersen et al. [6], fragmentation is becoming more prominent in IoT development process. In order for the software practitioners to conveniently build applications for IoT devices, there is a need for defragmentation and an interoperable open source generic software platform [6]. Openness in IoT will help the development community to develop software faster by not re-inventing the wheel. Openness in IoT is about open standards and interoperability, open source communities, open access to research data, open access to shared user data, open API, etc. [23]. Open data and Open API's are needed in order to share data collected by sensors with the application development community [33][34]. Trends shows growing number of open operating systems specifically designed for IoT, e.g. Contiki [44] which connects low-cost, low-

power, memory constrained things with the IoT systems. Even though open systems offer multitude of benefits for SW development there lies a greater responsibility on the vendor using the open source solution in order to ensure security & privacy of the IoT device [42].

Although there exists many benefits with use of open IoT systems, however, security is not guaranteed [25]. Security vulnerabilities can lead to privacy violations, monetary loss, malware and ransomware [6], other crafted security attacks (section 4.3), even loss of life e.g. by controlling hacked autonomous vehicles. Boddy et al. [8] in their F5 lab report has pointed out that IoT devices are easy to exploit and highly exploitable targets. The sum of attack points where malicious user can try to attack the IoT system, i.e. attack surface or attack vector grows as the number of connected devices increases [2]. Enormous amount of data transfer happens in IoT systems. Some of this data is personal, e.g. health information, contact information, IP address, GPS location etc. and some is secretive in nature e.g. bank account details, credentials, etc. This implies strong need for data security and data privacy mechanisms. Existing methods to handle security & privacy might not be applicable always due to various differences between IoT systems and legacy systems [7][40]. Thus addressing security & privacy concerns in IoT is utmost important task even though it might be difficult to achieve [31]. Security is usually ignored by IoT practitioners due to various reasons for example lack of security expertise, cost-savings and time tradeoff etc. IoT practitioner's takes reactive approach in mitigating security issues instead of proactively building security into the product from start.

1.2 Motivation

In the fast growing IoT industry there is a need for software development tools and platform that can enable faster, easier and convenient application development. Open systems is a solution to address above mentioned challenges in IoT. Openness helps in addressing the issues regarding interoperability and standardizations. A community maintained open source software is the most powerful tool since it evolves quickly and is maintained by hundreds of experts in the industry (Appendix E). It is cost-effective. It provides timely upgrades and security patches. Open source provides platform for invention and innovation. Hence, it is motivated to use an open IoT system which is

Flexible, i.e. easy to deploy in different user context [4]; Customizable, i.e. provides customizing features in the product in a cost-effective way [4]; Extensible, i.e. allows easy integration possibilities with other systems and tools [4].

With growing number of smaller IoT vendors, who does not have software security as core competence, throws a bigger threat on security & privacy of IoT devices running in special operational environments [42]. As an example, if a traditional hardware manufacturing company enables internet connectivity on their product, they can easily accomplish this with small group of SW developers. They might not necessarily have competence to do threat modelling, security reviews and might also lack security processes and audits. The result is a poor quality system that could be easily exploited by hackers and malwares due to a number of security bugs it might contain.

As seen earlier, IoT devices are highly exploitable targets and are easily exploited. The number of security attacks happening in the IoT domain is rapidly increasing due to various limitations in implementations and rapidly growing technology [3]. The details of these are presented in section 4.3. It is usually very expensive to handle security after solutions are deployed especially in constrained domains like IoT [31]. Hence, it is utmost important for IoT practitioners to securely design open IoT systems with right architectural approach and in right phase of SW development process. The first step towards addressing security & privacy within open IoT systems is to identify and analyze existing trends & challenges in handling security & privacy within IoT. Next step is to identify the design aspects that practitioners needs to consider when implementing an open and secure IoT systems.

1.3 Goal and Research Questions

Figure 1 Open Secure IoT System

Motivated by the openness trends in IoT domain and various security challenges that exists in the IoT domain, there arises a need to design an open IoT system that is secure.

Such a system should consider security at its heart rather than handling security issues reactively. We call such an IoT system as "**open secure IoT system"** throughout this report.

Thus, the main goal of the thesis is as stated below,

Goal: To provide insights for IoT practitioners in order to improve security & privacy design for an open secure IoT system.

Considering the rapid pace at which IoT technology is evolving, the amount of personal data being transferred between connected devices in small amount of time and growing number of attack surfaces & attack vectors, emphasizes the importance of the goal. The focus of this research is on security & privacy aspects of open secure IoT systems. In order to address the goal, first we need to understand if existing security & privacy mechanisms available from IT and internet world can be applied to IoT systems. Hence, RQ1 is formulated. Further, we need to identify gaps in such implementation and then contextualize a security model that needs to be applied on IoT software development life cycle. This will be addressed with the help of RQ2.

In order to fulfil the goal following research questions are identified and formulated:

RQ1: What are the trends & challenges in using existing security & privacy mechanisms within Internet of Things?

RQ2: What are the design aspects that practitioners needs to consider when implementing open secure IoT systems?

Above questions must be answered in order to fulfill the thesis goal. These questions will be answered both theoretically and empirically in details in chapter 4, 5 and 6. For identification of trends & challenges, both semi-systematic literature study was performed and interviews with industry experts were conducted. While discussing the security & privacy related challenges a broad view of the IoT has been undertaken. Instead of focusing on a particular domain within IoT, e.g. smart home, smart cities etc., this research focusses on IoT industry in general since outcome of the research will be applicable irrespective of a particular domain. This is further clarified in chapter 6 and 7. For identification of design aspects for open secure IoT systems, results obtained from

theoretical perspective were validated using results obtained from empirical interviews conducted with IoT industry experts.

The aim of this thesis is not just to aggregate evidences on decided research questions but also to support the design of open secure IoT systems for practitioners. This thesis presents the gap between the academic research conducted on security & privacy of IoT and industry best practices.

In order to fulfil the goal and address the research questions, the specific methodological approach described in chapter 3 is used.

1.4 Thesis Overview / Structure

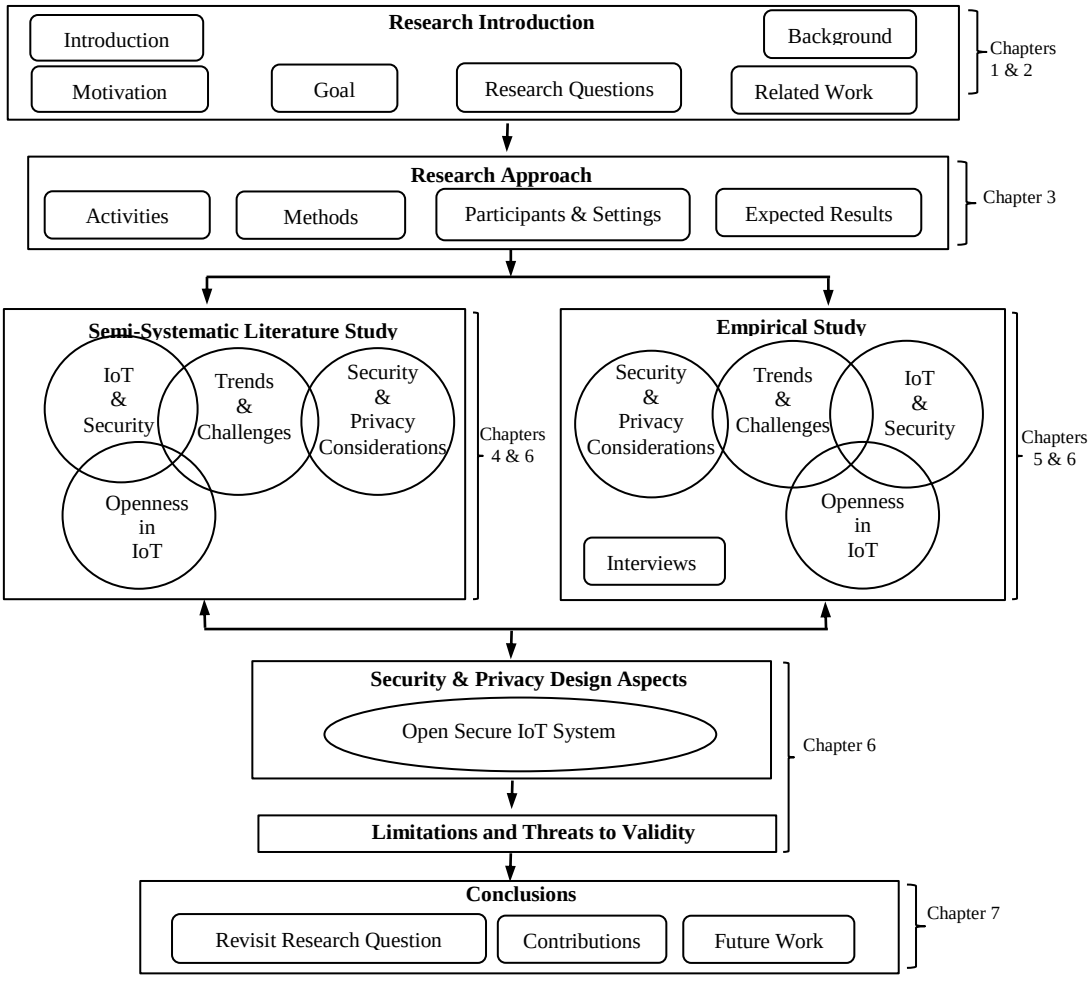

Figure 2 Thesis Organization

This thesis is organized into various chapters.

Figure 2 depicts the organization of the thesis into various chapters. Chapter 1 provides introduction into the area of Internet of Things and security & privacy. It addresses the research problem, research goal and the research questions to be answered. It also provides motivation and main contributions of this study. Chapter 2 provides background into the field of IoT, Open IoT systems and security & privacy. It also presents the related work done in the area of IoT security & privacy. Chapter 3 describes the research approach, the method used and the activities performed during the research. Chapter 4 presents the results of theoretical study performed during the thesis using semi-systemic literature study as the method and introduces to our open secure design approach for IoT. Chapter 5 is dedicated to the validation of theoretical understanding and presents results of the interview conducted with experts and practitioners in the field of IoT. In Chapter 6, the research outcome of the thesis is discussed considering the theoretical understanding and interviews conducted with practitioners. This chapter presents the gap between the research and industry in terms of IoT. It also presents the limitations and threats to validity. Chapter 7 presents the main conclusions, i.e. answering the research questions, main learning and possible future work that can be performed.

2 Background and Related Work

This chapter presents an overview of the foundation of the thesis. This chapter helps in identifying the research challenges and related work. This chapter provides elaborated introduction to IoT security and openness trends evident in IoT system that this research deals with.

2.1 IoT and Security

IoT is a very popular term of this decade. IoT has been defined differently by different groups. However, none of the definition seems to cover the complex nature of IoT systems [33]. It has been observed that IoT systems and applications are implemented in various domains ranging from personal and social domain [7] [35][38][39][40] to smart cities [35][7]. IoT devices can be found in automobiles [7][34][37][39], habitat and environment monitoring [31][34][35][38], smart home [7][31][40], smart grid, i.e. energy management [7][35][39][40], smart manufacturing [7] [35] [36] [39] [40], healthcare [7] [34] [35] [36] [37] [38] [39] [40], smart appliances [7] transportation [35] [37] [38], logistics [34] [35] [38] and smart office [38].

IoT systems and devices are characterized by various properties. They have ability to communicate [31][32], they are locatable [31] and autonomous [28][32] [35], they can sense physical phenomenon and perform computation [32]. These systems are also flexible [37][40], scalable [32][34][39][40] and heterogeneous [31][32][35][39][40]. Due to operational nature of IoT devices, they exhibit various constraints like limited computational power, limited memory and limited power [7] [35][39][40].

IoT and security are tightly connected and it is hard to treat IoT without considering security. This connection is largely due to the nature of the data handled and processed by the IoT systems. As the number of connected devices are growing the attack vector is also growing [2]. Traditional mechanism to protect devices from public network are available but needs rethinking when applied on the IoT systems and devices. The IoT practitioners need to consider similar security aspects as like the traditional systems when designing and implementing the IoT systems and applications. These security considerations includes Trust management [32][35][39][40], Authorization [39][40],

Authentication [32][39][40], Identification [10][35][40], Access control [10][35][40][39], Network security [40], Standardization and Security interoperability [35] etc. Digital divide [12] exists among IoT users based on their understanding of security & privacy risks. The three important privacy considerations include protection of personal data [35] [35] [39] [40], protection of sensitive data [10] [35] [39] [40] and protection of enterprise data [35][40]. Many challenges exists in using existing security & privacy mechanisms which are related to resource constraints, heterogeneity, privacy, software upgrades and operational environment.

2.2 Openness in IoT

Openness is a higher order concept characterized by access to information and other resources, collaborative participation, transparency of resources and actions, and finally opening up or making it non-exclusive [21]. Openness in software industry is about open standards, interoperability, open source communities, open access to research data, open access to shared user data, open API, etc. [23]. It is very much applicable in IoT context where millions of interconnected things produce enormous data that can be used in various applications like machine learning, data mining etc. in order to provide users with useful information and decisions. Various open OS are available in IoT domain e.g. Contiki [44], MindSphere [45], RIOT [46], Brillo [47], Mbed OS [48], Tiny OS [49], Free RTOS [50], UClinux [51], µC/OS [52], Lite OS [43]. According to Buckley et al. [22], "Software systems are open if they are specifically built to allow for extensions. Open systems usually come with a framework for facilitating the inclusion of extensions". This definitions highlight the very important characteristic of open system, i.e. Extensibility and Customizability [4][22]. New interfaces are been added to IoT systems that were never originally designed to have them and this creates potential security issues at cost of openness [42].

In order for developers to build applications for IoT devices in an easy, convenient and fast manner, there is a need for defragmentation and an interoperable open source generic software platform [6]. Openness in general offers opportunity for innovation and prevent developers from re-inventing the wheel.

There exists multiple IoT Architecture as already discussed by Vogel et al. in their paper [4], e.g. SOA, cloud based architecture, IoT ARM, etc. Other kinds of architectures that are mentioned in academic literature are WSN middleware [32] [37], object centric architecture where smart objects are central to the system [37], internet centric architecture [37], user centric open architecture which shows characteristics like flexibility and scalability [37][4]. An open architecture is an approach that helps designers, developers, and domain experts when considering products as a collection of services that can easily and flexibly be integrated, customized and extended. Vogel et al. [4] suggests an open architecture for heterogeneous and dynamic IoT environment where both the nodes and its interconnection can change dynamically. This open Architecture has characteristics like flexibility, customizability and extensibility. Each of these characteristic has their own associated properties. Author advocates that open architecture design principles is suitable for fast evolving IoT platform where both stakeholder requirements and stakeholders themselves change dynamically.

2.3 Related Work

Even though both security and IoT has existed for many years, however, none of the surveys that had been conducted during past has provided detailed study of security concerns related to the Internet of Things [35]. Many surveys have been published recently in the area of IoT and more specifically IoT security and privacy, i.e. [4], [5], [7], [32], [35] and [39]. All of these surveys have definitely highlighted on one common aspect, i.e. constrained environment and rapid growth of IoT technology.

Fernandez et al. [7], have described various challenges that exists in using existing security mechanism. Their analysis is based on four layered IoT architecture consisting of hardware, system software, network and application layers. They also emphasize that a cross-layer co-design approach is needed in order to address many of these challenges. The author did not discuss challenges in depth and validation techniques were missing for the proposed solution. Miorandi et al. [32], have provided a very simple and generic understanding of IoT, i.e. anything that connects or communicates with anyone, i.e. user or thing, at any moment of time and ubiquitously (anywhere). They have identified three main security challenges related to data confidentiality, privacy and trust. They did not

looked at other aspects of data security and privacy, e.g. authentication, authorization, anonymity and heterogeneity. Arbia et al. [35], have presented systemic and cognitive approach addressing identification, access control, trust and privacy. They have emphasized on the presence of person and intelligent things in their contextual model of IoT. They have not addressed the open systems architectures prevalent in IoT domain. Sicari et al. [39], have presented challenges in using existing security measures due to heterogeneity property of IoT systems. They have also described that the key security requirements include authentication, confidentiality and access control. Vogel et al. [4] [5], have addressed the needs of IoT system by using open architecture. The key characteristics of open Architecture includes flexibility, customizability and extensibility so that the system can easily evolve over time. However, Security & privacy is completely missing in their approach. In addition, they have not considered important properties of IoT systems like interoperability, heterogeneity, autonomy and mobility in a more exclusive way

Based on previous researches, it can be seen that many security & privacy related challenges exist in constrained, heterogeneous and rapidly growing IoT domain. These challenges lead to various security requirements e.g. authentication, authorization, confidentially, etc. Also, various architectural styles can be used to address IoT systems design e.g. systemic and cognitive, open architecture, etc. However, none of these reports gives full overview of different kinds of security & privacy related challenges that exists and how to address them during the early phase of software development lifecycle.

Various academic research has been conducted in the area of IoT security & privacy [Studies: S2-S11] in order to address security & privacy within IoT domain. Industry initiatives like IoT Security Foundation exists with a mission to help secure IoT [2]. Despite these efforts, no significant improvements are visible in the area of security & privacy within IoT industry or specifically within open IoT systems and there are several open challenges to address as seen in our related work above.

3 Research Approach

This chapter starts with the research approach that is chosen for research study. It provides details regarding the associated activities and methods used during the research work. It introduces us to various participants and settings involved during the study. It concludes with section describing the expected results for the research work.

3.1 Approach

The main research goal is to provide insights for IoT practitioners in order to improve security & privacy design for an open secure IoT system. It provides a good opportunity to use qualitative methods in order to collect data, analyze and validate results. Qualitative method is used as a method of data collection because this research study is based on "what", "why" and "how" questions but not on "how much" or "how many" types of questions. Although, empirical research methods are widely used in academic researches, there is very little advice or information available on which methods are suitable and shall be chosen for which research problem [13]. It is suggested to use multiple approaches using multiple methods [13]. In this research, both semi-systematic literature study and interview methods are used to collect data for answering the defined research questions. In order to achieve thesis goal and address research questions, interpretative insights and empirical evidence are provided in this study. Various activities that were performed for the selected research approach are presented further in this chapter.

3.2 Research Activity - Semi-Systematic Literature Study

In order to identify valuable, informative and relevant research in the domain of the study and the topic that is explored during the study, systematic literature review is usually performed from the initial stage of research [9]. The semi-systematic literature study was performed based on the guidelines for systematic literature review (SLR) for software engineering as proposed by Kitchenham et al. [23]. The participant of semi-systematic literature study was current researcher only. Supervisors helped with review of the report and other needed guidance. However, this study does not fulfill all criteria

proposed by Kitchenham et al. [23]. In particular, the criteria that were fulfilled are design and documentation of search string and search process, usage of electronic database for initial search, usage of inclusion and exclusion criteria, performing quality assessment, usage of data collection form. The criteria that were not fulfilled are, more than one author review and evaluate the paper, detailed data extraction and data synthesis. Also, some papers, e.g. open architecture related were preselected and were not found through the defined search process. Hence, the SLR performed here is called a semi-systematic literature study.

The semi-systematic literature study resulted in identifying the latest trends & challenges in using existing security & privacy mechanisms on IoT. It further resulted in identifying design aspects that practitioners need to consider when implementing open secure IoT systems.

3.2.1 Method

Semi-systematic literature study method is selected in order to get fair evaluation of approaches used to handle security & privacy in IoT domain. The semi-systematic literature study was performed based on steps as shown in Figure 3.

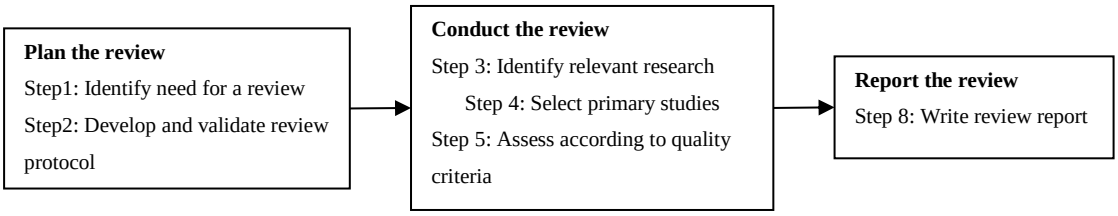

Figure 3 Semi-Systematic literature study process

A semi systematic literature study was performed to identify key issues in the existing researches relevant to the domain of study. The steps even though listed as a sequence were actually performed in iterative manner [23]. The problem domain was defined for the topic of study and search was conducted on literature that is available related to the study. The need for performing the review was identified by systematically identifying and reviewing existing work in the domain. The research goal and research questions were formulated. The semi-systematic literature study was performed in relation to the

research goal and research question [9]. Review protocol was defined as described further in chapters 3.2.2 - 3.2.6.

3.2.2 Search Process

A manual search is more detailed and produces better results compared to automated search even though it requires high efforts. Manual search was done using 16 premium online published journals and 9 premium conference proceedings related to IoT, security & privacy in order to optimize the literature selection process. These journals and conferences were selected based on the inclusion and exclusion criteria as defined in later sections. Specific sources for target search were used in order to avoid low quality research papers. The selection results are shown in **Table 1** and **Table 2**.

Table 1 Searched Journals

ID	Journal
JNCA	Journal of Network and Computer Applications
JDCN	Journal of Digital Communications and Networks
JCC	Journal of Computer Communications
JCIS	Journal of Computer and Information Sciences
JSS	Journal of Systems and Software
JAHN	Journal of Ad Hoc Networks
JCN	Journal of Computer Networks
JFGCS	Journal of Future Generation Computer Systems
CLSR	Computer Law and Security Review
FGCS	Future Generation Computer Systems
IEEESP	IEEE Security & Privacy
JISA	Journal of Information Security and Applications
BH	Business Horizons
JIS	Journal of Information Sciences
JCS	Journal of Computer and Security
IJNSA	International Journal of Network Security & Its Applications

Table 2 Searched Conferences

ID	Conference
ECSA	European Conference on Software Architecture
ISOCC	SoC Design Conference
IEEE Big Data	IEEE International Conference on Big Data
I-SMAC	International conference on IoT in Social, Mobile, Analytics and Cloud
TENCON	IEEE Ad Hoc Networks
W3CWOT	W3C Workshop on the Web of Things
EuCNC	Networks and Communications European Conference
CCWC	Computing and Communication Workshop and Conference
COMPSAC	IEEE 38th Annual International Computers, Software and Applications Conference

Searched journal and conference proceedings were manually reviewed in stage 1 as shown in Figure 4.

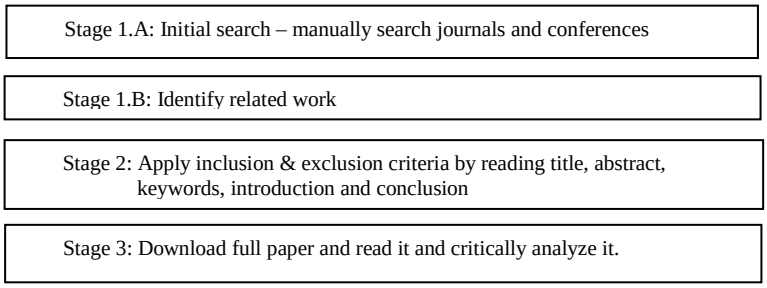

Figure 4 Literature search process

The keywords used in search process were “security for IoT”, “privacy”, “security threat” and “IoT”. This resulted in 3364 papers searched. Their title were read for relevance to the topic of study, goal and research questions. This reduced further reading significantly. Further refinement was done by excluding all results that were older than year 2000 due to the fact that IoT is a very modern concept that started almost a decade ago. Also, security is an ever evolving field and it is more relevant to study security related literature that is latest and relevant to IoT. Next stage was to read the abstract and then if the paper satisfied selection criteria, further reading included introduction and conclusion. This stage concluded with 35 papers for data collection. Because IoT is not a mature domain and in order not to miss any relevant literature, any existing literature that

included either empirical, theoretical, conceptual or literature surveys were selected. Then in next stage studies were identified in related reviews, namely [4][5][7][32][35] and [39]. In stage 2, inclusion and exclusion criteria were applied on the selected studies by reading introduction and conclusions. In stage 3, full text of the selected studies were obtained. After reading the full text of the selected studies, the final inclusion and exclusion decisions were made.

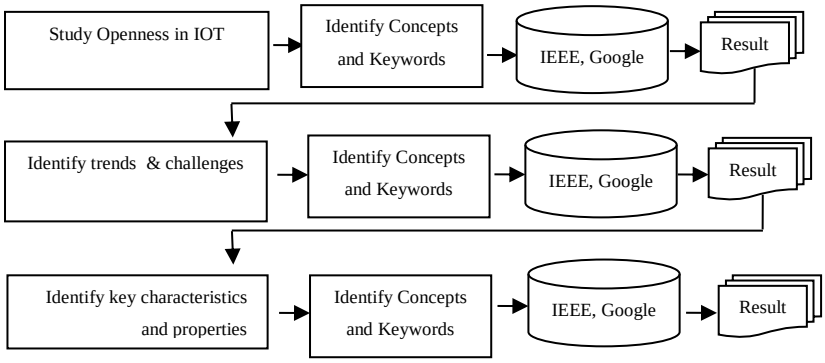

Figure 5 Literature Selection Process

A step wise literature selection process was used in order to address the research question appropriately. On every step a particular goal or problem area was studied and results obtained from that step were applied on to the next step. This helped us navigate to the desired results in a more structured and optimized way. The literature selection process described in Figure 5 started with step 1 as study of Openness in IoT. The focus was on in-depth study of openness in IoT, open source methods and open architecture for IoT. Search was conducted using "Open Architecture", "Open Source" and "Openness in IoT" as keyword. Existing keywords and concepts were identified in the domain of study that helped to identify criteria for further search on the literature. Using the identified keywords, search was conducted on resource databases. Results generated from current step are used to set the criteria which are used in further searches in an iterative manner. In step 2, keywords like "security for IoT", "privacy", "IoT" and "security threat" were used to identify key trends & challenges in using existing security & privacy mechanism and at the same time identify key security & privacy related requirements. The literature selection process concluded with step 3 as identifying security & privacy related characteristics and properties for IoT.

3.2.3 Inclusion and Exclusion Criteria

Since the topic of research is very popular and lots of material is available in security & privacy domain, it was important for us to define inclusion and exclusion criteria. These criteria helped us to identify the relevant studies that were directly addressing our research question. Inclusion and exclusion criteria were applied on every step of the search process. A paper that satisfied all inclusion criteria (Table 3) was selected for final study and the paper that met any of the exclusion criteria (Table 4) was excluded from selected list.

Table 3 Inclusion Criteria

#	**Inclusion criteria**
1	Study is of high quality and comes from renowned and acceptable sources.
2	Study addresses challenges or constraints in IoT domain.
3	Study addresses challenges or constraints in using existing security & privacy mechanism in IoT domain.
4	Study explains or is related to IoT architecture.
5	Study addresses security threats in IoT domain.

Table 4 Exclusion Criteria

#	**Exclusion criteria**
1	Study does not come from renowned source or study is an editorial, abstract, short paper, poster, summary, keynote, conference summary, abstracts that do not provide enough information related to research paper, etc.
2	Study concerns security & privacy in general and is not related to IoT.
3	Study that are relatively old, i.e. before year 2000.

3.2.4 Quality Assessment

According to Kitchenham et al. [23], it is crucial to assess quality of the primary or selected studies. The following questions based on recommendations by Kitchenham et al. [23] were used to assess quality.

Q1: Are the inclusion and exclusion criteria described adequately?

Q2: Is the research context and research design clear?

Q3: Has the author critically examined their findings, potential bias?

Q4: Has the author recommended further research?

Scoring was given to each question +1 (yes), 0 (to some extent), -1 (no) the sum of the score of all the questions define the quality of reporting of the study. These scores were used to identify the quality of the study and not as an inclusion or exclusion criteria.

3.2.5 Data Collection and Analysis

The data collected from each study is listed in the below Table 5. Fields 1-6 were collected for documentation purposes. RQ1 was addressed using fields 7-9 and RQ2 was addressed using 7, 8, 10 and 11.

Table 5 Data Collection Template

#	**Data**	**RQ**
1	Year	n/a
2	Title	n/a
3	Author	n/a
4	Source: Journal/Conference	n/a
5	Keywords	n/a
6	Abstract	n/a
7	Main topic area	RQ1, RQ2
8	Research Question	RQ1, RQ2
9	Constraints in using existing security & privacy mechanism	RQ1
10	Key points w.r.t security in IoT	RQ2
11	Key points w.r.t privacy in IoT	RQ2

The collected data was stored in a spreadsheet. According to Kitchenham et al. [26], aggregating the data can be done easily using tabulation technique. Data from studies were assembled and examined to answer the research question. Instead of using meta-analysis, data was manually reviewed from the spreadsheet [27].

3.2.6 Deviation from Protocol

The type of study for each paper was excluded since the intention was to include all study types. In addition, open architecture related papers [4][5] were preselected in this study as a main motivation that drives this research.

3.3 Research Activity - Interviews

'Qualitative interviews' is a powerful research tool and an excellent method for collection of data used in various research from past [17]. Interview method is very appropriate and applicable to answer research question and goal mentioned in this work. Interviews were used for validating the results obtained from semi-systematic literature study. Interviews were conducted with experts & practitioners within IoT domain using seven stages as defined by Kvale et al. [18]. In *Thematizing* stage, "what" and "why" types of questions are defined. In *Designing* stage, interview questions were designed based on the goal of the study and research questions to be answered. In *Interviewing* stage, interview guide was prepared and interviews were conducted based on interview guide for collecting data. In *Transcribing* stage, the interviews were transcribed from recorded audio into tables which are available in appendix A-F. In *Analyzing* stage, analysis of the transcribed interviews was done using open coding technique as suggested by Creswell [16]. In *Verifying* stage, quality parameters such as reliability, validity and objectivity were used in order to improve the quality of the collected information and data. In *Reporting* stage, the prime focus is on ethical issues in studying research. Hence, the results of the interviews were made available as a report for readers in a readable format.

According to Patton [19], informal conversational interviews, semi-structured interviews and standardized open-ended interviews are the three types of qualitative interviewing methods. However, semi-structured interviews are widely used technique. They are dynamic in nature, i.e. does not expect respondents to answer sequentially and at the same time interviewer can follow the defined procedure [15]. In this study, face-to-face interviews were conducted for best results [18].

3.3.1 Thematizing and Designing

It is crucial to get views and opinion of the expert in the field with varied roles and responsibilities who are working on delivering smart IoT products to billions of users around the world. Interview with IoT practitioners can bridge the gap between theoretical understanding and developed model for open secure IoT system.

As described by Kvale et al. [18], 'How', 'What' and 'Why' kind of questions are asked in a semi-structured interview. In this study, 'Why' kind of questions were used for defining purpose of the study. 'What' kind of questions were used to get the understanding of the respondents on the field of the study and respondents opinions on the research questions. 'How' kind of questions were used to analyze the subject matter. In this study, simple and brief questions were designed built upon the research questions and our open secure design approach for IoT.

3.3.2 Interviewing

Questions were asked to the interviewees as defined in the interview guide. However, based on the responses existing questions were modified or new sub-questions were asked during the interview. This provided flexibility and dynamism in the interviews in order to gather as much of relevant information needed for answering the research question [18].

3.3.2.1 Selection of Interviewees

The research relies on the data gathered primarily from companies within IoT domain in southern part of Sweden. These companies produce IoT solutions, including but not limited to IoT hardware device, cloud based services, security solutions, customer support, etc. The interviewees were selected based on varied roles they have in their organization in order to get variety in the responses. In case if the selected role was not available an alternate person was approached from the same organization or a new organization was selected. The selected roles are relevant to the topic of research and best suited for gathering data related to both the research questions since they handle design & development of various security solutions within IoT and outside IoT domain. Moreover, most of them are the key decision makers within their organization including security decisions and budgets. They also follow latest security trends in IoT industry. They deal with various security & privacy related challenges in their operations. The details of respondents are kept anonymous in order to respect privacy of the participants and bring anonymity to the responses. Hence, each interviewee is mapped to an acronym as a way to refer them in later chapters. The interviewees are classified according to their role, organization and domain in Table 6.

Table 6 Interviewee Role Mapping

Respondent	Role	Organization (Domain)
SM1	Security Architect	Sony Mobile Communications AB (Mobile Coms.)
SM2	Senior Architect - IoT	Sony Mobile Communications AB (IoT Solutions)
TS1	Technology Leader	TechSource AB (Industry Automation)
SN1	Technology Expert	Sensative AB (Home Security)
AX1	Security Coach	Axis AB (Home Surveillance)
HS1	Security Expert	Hyker Security AB (Data Security)

3.3.2.2 Conducting pilot interview

A pilot interview was conducted with respondent SM1 in order to validate the interview guide and kind of responses obtained. Once the researcher was satisfied that the interview guide is generating expected results follow up interviews were conducted with other interviewees as listed in 3.3.2.1. Pilot interview also facilitated in measuring approximate time it takes to conduct other interviews and follow up interviews were scheduled accordingly. It also helped in testing the tools and technique used in conducting and analyzing interview, e.g. audio recorder, transcriber, etc. SM1 was chosen for pilot study since this candidate was easy to approach and was available. SM1 has more than a decade long experience working with security SW and architecture which makes him suitable for our pilot study.

3.3.2.3 Conducting interviews

According to Kvale et al. [18], in person interviews are most efficient, reliable and authentic. As an alternate method, telephonic interview or video-conferencing could be used if in person interview is not at all possible [18]. Interviews were conducted face-to-face based on the availability of both interviewee and interviewer.

Initial contact with the interviewees was established by contacting them over email or linked-in. The content of the email contained clearly stated purpose of the interview and the domain or area of research study and also abstract of the semi-systematic literature study report. It also included the goal of the research study. A meeting was scheduled

once confirmation of the interview request email was received. Interview guide was provided in order to remove any ambiguity, mistakes and also, unethical issues if any, could be addressed well in time. If there are any findings, it will be easier to update interview guide rather than ending up with an interview that cannot receive legal clearance of the organization.

A summary of the interview was sent to the interviewee on completion of the interview for confirmability, i.e. review and approval. Once approval was in place, process of analyzing, verifying and reporting followed [18]. In case if interviewees show interest in thesis report or presentation, it will be shared after seeking approval from thesis supervisor.

3.3.3 Transcribing and Analysis

Transcription is a method in which oral interviews are converted into written text [18]. Audio recorder was used to record the whole interview, which is a common way according to Kvale et al. [18]. Usage of audio recorder enables interviewer to focus on the interview and concentrate on the topic. At the same time, interviewer can analyze the recordings later on by replaying the audio multiple times. From the audio recordings gathered during data collection step, text transcriptions were created. According to Creswell [16], a consensus was established prior to the interview with regards to anonymity and recordings of the interview. Audio recordings were played multiple times in order to remove any ambiguity or misunderstanding of the information presented by the interviewee.

Appropriate tools were used to compare data obtained from various interviews. This helped in accurate analysis of the obtained interview data. An empirical investigation was conducted using the research questions and theoretical model, i.e. our open secure design approach for IoT. Analysis of the interviews was done using open coding technique. Open coding technique is a neat way of categorizing data obtained from the qualitative interviews [15] [16]. Interview guide was used to perform coding of the interview taking into consideration the theoretical model, i.e. our open secure design approach for IoT. Open coding technique helped in understanding the interview results from a practical and realistic perspective. It also helped in creating deeper understanding of the subject matter.

3.3.4 Verifying and Reporting

Quality of qualitative research is one of the most important criteria. It includes validity, objectivity and reliability of research method [20]. **Validity** means that interview should produce valid knowledge that is true and correct. In order to get the expected results and remove any scope of misunderstanding that might result in improper results, all the needed and relevant information was conveyed well in advance using email. Interview guide was provided prior to the interview so that the interviewees get well versed and participate mutually in the interview. **Objectivity** means that the interview conducted are free of bias and influence. Researchers are not supposed to influence interviewees and interrogate them as they are [18]. Research ethics should be followed as suggested by Creswell [16], i.e. to avoid bias or influence the interviewee. Utmost care was taken in order to avoid bias by providing relevant and needed information about the interview, its purpose, motivation and goal of the research study. Providing interview guide prior to interview also helped in reducing bias. Also, participants were chosen from startups to big organizations. These organizations represented different domains within IoT, e.g. Home security, surveillance, Mobile devices, Industry automation etc. Participants had different roles within their organization, e.g. Senior Architect, Security Architects, Technology Expert, Technology Leader, Security Coach, Security Expert, etc. Introducing these variation helped in further reducing bias to a greater extent. **Reliability** means that the research creates same observations of a given phenomenon when similar research methods and procedures are used [11]. Reliability in the interview was achieved by validating the data collected during interview against audio recording. Peer review, supervisor feedback and review by industry practitioners helped in creating reliable report. The variation in selection of participants helped in cross validation of obtained data by different participants producing reliable research work. In order to establish trust and follow organizational policies, interviewee consent was requested in order to use the organization name in the report. Also, interview transcripts were sent in order for them to review and highlight any sensitive information that should be removed from analysis.

4 Semi-Systematic Literature Study

In this chapter, the results of the semi-systematic literature study were summarized. The results are related to inconsistency in definition of IoT, properties of smart thing, properties of IoT system, constraints in IoT system and various available architecture. Also described are, possible security attacks on IoT systems and devices, various security & privacy considerations, challenges in using exiting security mechanisms and openness trend that is prevalent in IoT.

4.1 Search Results

3364 papers were manually searched as evident from Table 7 below covering various sources identified based on inclusion and exclusion criteria. The number of papers after stage 1 were 34.

Table 7 Data Search Result

Source	Papers hits	Paper after stage 1
IEEE Xplore	25	8
Science Direct	3335	22
ACM Digital library	2	2
W3C	1	1
arXiv	1	1

Papers that were not relevant to the research questions were excluded during data collection phase. This resulted in 11 papers for final review listed in Table 8.

Table 8 Studies Included for Final Review

ID	Title	Author	Date	Type
S1	An Open Architecture Approach: Towards Common Design Principles for an IoT Architecture	Vogel et al. [4]	2017	Conference
S2	Security, privacy and trust in Internet of Things: The road ahead	S. Sicari et al. [39]	2014	Journal
S3	Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?	Fernandes et al. [7]	2017	Journal
S4	Internet of things: Vision, applications and research challenges	Miorandi et al. [32]	2012	Journal
S5	Data Privacy for IoT Systems Concepts, Approaches, and Research Directions	Bertino et al. [35]	2016	Conference
S6	A roadmap for security challenges in the Internet of	Arbia et al.	2017	Journal

	Things	[35]		
S7	A framework for automating security analysis of the internet of things	Mengmeng et al. [31]	2017	Journal
S8	Internet of Things (IoT): A vision, architectural elements, and future directions	J. Gubbi et al. [37]	2013	Journal
S9	Privacy and Trust Relations in Internet of Things from the User Point of View	Ismail Butun [40]	2017	Conference
S10	SecKit: A Model-based Security Toolkit for the Internet of Things	Neisse et al. [12]	2015	Journal
S11	Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm.	Atzori. et al. [33]	2017	Journal

4.2 Internet of Things (IoT)

After doing an extensive study of the identified and selected journals and conferences, several key study areas within IoT were identified that are described in the following sections. Firstly, it is important to gather general understanding i.e. IoT definition, various properties of smart things, key features, properties and constraints of IoT. Then it is important to understand architecture of IoT. This will help us better understand the security challenges.

4.2.1 IoT Definition

As a first step of the semi-systematic literature study process, it is important to understand the term "Internet of Things" which has been defined differently by different sources. Various definitions of IoT were encountered in the literature. Even though much work has been done in the field of IoT, there exists inconsistencies in understanding internet of things concept. The term Internet of Things was first coined by Kevin Ashton [37]. Table 9 enlists various definitions identified from the semi-systematic literature study process.

Table 9 IoT Definitions

Source	Definition
Original term by Kevin Ashton [28]	IoT is about "enabling computers (therefore, internet) to observe, identify and understand the world – without limitations of human-entered data"
IERC, "Internet of Things," 2014. [30]	''A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated

	into the information network"
Widely used by RFID Group [14]	The worldwide network of interconnected objects uniquely addressable based on standard communication protocols.
Atzori et al. [33]	"a conceptual framework that leverages on the availability of heterogeneous devices and interconnection solutions, as well as augmented physical objects providing a shared information base on global scale, to support the design of applications involving at the same virtual level both people and representations of objects."
Gubbi et al. [37]	Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with Cloud computing as the unifying framework.

The first three definitions were selected from sources that are most commonly used within the IoT industry. Last two definitions were taken from the paper selected for final review (section 4.1). However, none of the definition is satisfactory enough.

4.2.2 Smart Thing

A smart thing is usually an end point or node e.g. a sensor that collects useful data and send data for further processing to cloud or other smart objects [32]. Example, thermometer, heart monitoring implants, sensors in autonomous-cars, etc. During the semi-systematic literature study, various properties of smart things has been identified which are listed in Table 10 Key properties of smart thing. These properties are also applicable to IoT systems since smart things are an integral part of IoT Systems.

Table 10 Key properties of smart thing

Property	**Ref.**
It is a **physical object** having physical features like size, shape, etc.	[32]
It can **communicate** with other parts of the IoT system, e.g. ability to be discovered, send/receive messages	[31][32][37]
It is **locatable**, addressable and can be **uniquely identified**	[31][32][37][40]
It is **autonomous** and hence does not need human intervention	[32] [35]
It can **interact** with environment, i.e. sense physical phenomena, e.g. light, sound, vibration, temperature, proximity, etc. and trigger actions (actuators)	[32]
It can perform basic **computation**, e.g. routers, NFC, RFID, etc.	[32]

4.2.3 IoT System Properties

During the semi-systematic literature study, various researchers have identified different properties or features that IoT systems and devices needs to support. IoT systems in general are **Open** [4][34][37] and **Flexible** [37][40]. They usually embed **Security & privacy** preserving mechanism [32][34][39][40] and have **Data management** capabilities [31][32][34]. These systems are **Heterogeneous**, i.e. they use various protocols, platforms, OS, devices, etc. [31][32][35][39][40]. They are **Scalable** [32][34][39][40]. IoT systems are built for **Energy-optimized** solutions [32].

4.2.4 IoT System Constraints

Much emphasis has been given on the constrained nature of IoT devices by all the literature that were studied i.e. S1-S11. The major constraints that has been pointed out by [7] [35] [39] [40] is the *limited computational power*, *limited memory* and *limited battery power* of IoT devices. These constraints are prominent due to the nature of IoT devices, associated costs and the physical environment in which they operate. IoT systems shows *fragmentation* [4] and exhibits *heterogeneity* [31] [32] [36] [39] [40] since they use various protocols, platforms, architectures, OS, etc. This significantly impacts the property of semantic interoperability and data management [31].

4.2.5 IoT Architecture

A full comprehension of the IoT architecture is needed in order to understand the security challenges associated with IoT systems. There exits various architecture for design of IoT systems. The most popular IoT architectures are based on SOA and WSN middleware [32] [37]. Other architectures that are mentioned are object centric architecture where smart objects are central to the system [37], internet centric architecture [37] and user centric open architecture which shows characteristics like flexibility and scalability [4] [37]. A simple four layered IoT architecture has been described by Fernandes et al. [7], **Hardware layer** contains sensors and actuators. **System software layer** contains IoT platforms that provide controlling software. **Network layer** contains elements that enables communication between smart things or

objects. **Application layer** consists of various applications needed in order to control physical processes.

Once initial understanding of IoT was gathered, i.e. definitions, key properties, architecture and key constraints. Next step was to understand security & privacy aspects, i.e. security attacks on IoT systems, security requirements and challenges.

4.3 IoT Security Attacks

Interaction with huge number of nodes increases the attack surface and can potentially lead to serious security problems. Due to heterogeneity, rapid growth of IoT industry and key constraints, as listed above, IoT devices seems to be the easy and highly exploitable target [39]. According to Bertino et al. [35], 25 vulnerabilities are recorded per IoT devices based on a study conducted by HP. These vulnerabilities range from weak passwords to unencrypted network traffic to vulnerable user interfaces and/or firmware. Some of the prevalent attacks are summarized from the studied literature in below Table 11.

Table 11 IoT Security Attacks

Active	**Passive**
DoS attacks [7] [31] [35], DDoS [7] [35]	Eavesdropping [7][32] [35][40]
Buffer overflow [34], SQL injection [35]	Traffic analysis [35]
Node capture and Node controlling [31], Masking [32]	Man-in-middle attack[35][39]
Message modification and/or alteration [35]	
Sybil Attacks [35], Proxy attack [35]	
Ransomware [7], Physical attacks [35]	

Since no high level security mechanisms can be implemented on passive RFID kind of devices, it opens up vulnerabilities by allowing tracking of person and smart things [37]. Hence, it is utmost important to secure IoT technology with right architectural approach and in right phase of system development.

4.4 Security & Privacy Considerations for Secure IoT System

As seen earlier, many constraints exists in IoT systems which potentially opens up opportunities for crafted security attacks on IoT devices. It was considered to survey the

key security considerations that an IoT system shall consider or address in their implementations. Many of the key security considerations from existing IT systems are also applicable on IoT systems that are described below.

Trust management is a fundamental issue [35][39][40]. It is critical to manage device trust, entity trust and data trust. **Access control** needs to be in place i.e. who should be allowed to access smart things or data generated by smart things [35][39][40]. This is achieved by providing identification [10][35][40] of smart things owners, authentication [32][39][40], authorization [39][40], non-repudiation [39][40] of data and revocation [40]. **Confidentiality** of data shall be accessed not only by authorized users but also by authorized smart objects or things, **integrity** and **availability** of data should be secured [32][39][40]. **Network security** should be ensured by providing confidentiality of the user and preventing eaves-dropping over the communication channel [40]. **Key management**, i.e. distribution of security key, key storage etc. needs to be considered [35]. **Hardware level security** should be used in order to prevent malicious components or instruction sequence from execution [7]. Hardware should be well tested before deploying since it is expensive to fix hardware related issues once product is shipped [7].

However, some new security requirements arises due to specific features or properties or nature of IoT systems. The **heterogeneity in security implementations** needs to be handled when smart things connect with each other [35]. **Autonomy** in handling security threats and taking preventive measures can be achieved by using cognitive and systemic approach as suggested by [35]. **Efficient security algorithms** that can be implemented in resource constraint IoT devices and networks needs to be designed and implemented [35]. As already understood earlier, IoT domain is highly fragmented hence there is a need to implement **standardized protocols** instead of using proprietary solutions in order to provide security interoperability, compatibility and extensibility.

Privacy is an important aspect in IoT domain due to the nature of data involved. According to Miorandi et al. [32], “privacy defines the rules under which data referring to the individual users may be accessed”. The amount of data that is collected by the IoT sensors is extremely large and is very private in nature, e.g. it may be related to personal activities, e.g. GPS locations by health loggers, daily activities logged by connected

wearables, home related information from smart home equipment's, etc. Such an information imposes critical privacy issues unless it is managed properly and according to user consensus [12]. Following privacy considerations that has been identified from the studied literature can be categorized into data privacy related and access privacy related.

Data Privacy related: Protection of personal data, i.e. when personal information collected by IoT devices is transferred to other entities, e.g. cloud for further processing [35][35][39][40]. PII shall be protected throughout its entire life cycle. **Protection of sensitive data**, similarly, any other sensitive or secret data shall be protected throughout its entire life cycle [35][39][40]. **Protection of Enterprise data** when IoT devices in enterprises could potentially capture information that can be further exploited with malicious intentions and hence must be protected [35][40]. Appropriate **cryptographic protocols** should be used in order to protect privacy of sensitive data. **Runtime intrusion detection** by profile based tracking of privacy-sensitive data in order to detect run-time anomalies can be implemented. **Data privacy solutions** must be implemented during all phases of data usage, i.e. collection, transmission and storage [35]. The operations includes but are not limited to data Authenticity, data aggregation, data anonymity, data pseudonymity, i.e. mechanisms shall be applied in order for IoT applications to work on anonymized data, data un-linkability and secure erase of memory in order to handle data privacy [35][40].

Access Privacy related: Data access control [38]need to be in place in order to control access to personal data during entire life cycle of data [35] [39]. **Contextual Access control**, e.g. location, temporal, etc. i.e. access to data can be blocked based on contextual information [35] [35]. **Access management** based on type of data [35]. **Digital divide** [12] exists among users based on their understanding of security & privacy risks. It is commonly understood that users with higher level of technical proficiency have better understanding of associated privacy risks. IoT systems should be designed in order to handle digital divide.

Smart objects are present everywhere in an IoT systems, at the same time there is risk of mishandling of the technology due to various reasons by intended or unintended users. Hence, it is crucial to address above mentioned security & privacy considerations [35].

4.5 Security Challenges

We have walked through various security & privacy considerations for IoT systems. Many of those are currently implemented using existing security mechanisms. However, there are various challenges in applying these mechanisms as identified from studied literature. They can be categorized as described below.

Challenges related to resource constraints: Existing security solutions, e.g. cryptographic algorithms, security tools, etc. needs reengineering before they can be used on a resource constrained IoT devices [32] [35]. Otherwise, new security solutions must be developed that are strong enough, cost-effective and have low energy consumption requirements [35]. Process isolation requires memory management units which are not available on constrained IoT devices [7]. Due to limited computational power on low power devices, application of hardware root of trust and hardware supported software isolation might not be possible or is challenging enough to be applied on. Due to limited communication and computing capabilities, it is very difficult to use full protocol stack on a device and applications doesn't provide end-to-end security [32].

Challenges related to heterogeneity: It is a big constraint to develop a generic security solution for heterogeneous IoT systems [35]. Existing network security mechanisms cannot be easily applied on IoT systems that uses diversified communication protocols and shows lack of maturity and standardization [36]. Multiple standards are available in IoT domains which creates confusion among practitioners and hence it poses risks of partial compliance of standards or not utilizing any standard at all in IoT systems [4]. Availability of multiple IoT platforms, OS options and use of many different programming languages creates fragmentation which poses various challenges in using existing security mechanisms [4]. Trust establishment and trust management in a heterogeneous IoT system containing enormous number of nodes is a challenge in itself [35]. Interactions among IoT devices occurs in a complex manner using many different security mechanisms and varied privacy policies [35].

Challenges related to privacy: Dynamic nature of IoT systems makes the existing mechanisms to protect data confidentiality inapplicable. This dynamism comes from amount of data involved and scalability issues as well from access rights changing at run time that are being applied to dynamic data [32]. Ubiquitous data in IoT systems pose issues related to privacy violations [32]. Conventional data protection mechanisms needs to be reconsidered during transmission and processing of data on IoT [36]. In IoT systems, it is not only humans involved but smart objects or things as well and hence managing user identity pose new issues even though it might be a well-known topic [32]. Identity-management solutions should focus both on intra-domain and inter-domain [40]. Conventional ACL's are not applicable due to its complexity and lack of flexibility [35]. Traditional systems were using controlled database systems with special interfaces to access stored data. However, modern IoT systems implementing cloud storage that pose new privacy concerns on data handling [36]. The communication between gateway and cloud is protected by use of network security algorithms. However, data transmitted within cloud and transmission from smart things must also be protected [40].

Challenges related to software upgrades: It might not be possible to update an IoT device due to absence of update channel [7]. It might be required to shutdown system in order to complete software upgrade process which is not practical in many IoT scenarios [7]. Software upgrades might trigger re-verification of compliance policies, e.g. in healthcare domain which is not a cost-effective and time-effective solution [7]. Updates on devices (e.g. computer upgrade) in tertiary network functions can lead to undesired effect on primary IoT devices [7].

Challenges related to operational environment: IoT devices runs in different operational environments, e.g. mobile users or devices, smart objects might be physically accessible to attackers, no trusted authority defined [35] [39] [40]. IoT devices connects with open and public network which imposes further security challenges [35][39]. Critical security problems arises when resource constrained IoT devices interacts with a large number of nodes which results in bigger attack vectors [37]. Multiple interaction modalities that exists on IoT devices results in a challenge to determine which authentication mechanism suits best [7]. In classical systems, trust establishment is done

in a centralized way. However, trust management in dynamic and distributed IoT environment is a challenging issue [35]. It is important to secure machine learning algorithms that are used to detect security issues in IoT systems. Some smart objects that are included in IoT systems might not be designed in order to be connected to internet. In such a case, these IoT systems might partially or fully be compromised [36]. Security unawareness among IT companies and by end-users or the cost associated with adoption results in lack of security technique adoption [36].

4.6 Openness in IoT

IoT software development shows emerging trends of openness, e.g. open standards are used on network layer e.g. IPv6 together with ZigBee, UDP, RPL, 6LoWPAN, etc. [35]. Open data and open API's are widely used in order to make best use of the data generated by sensors [33]. Atzori et al. [33] suggests open process in order to promote interoperability and reuse of services. IoT devices exhibits distinct features and constraints compared to traditional computing devices and hence trends shows growing number of open operating systems specifically designed for IoT systems (section 2.2). Even though open source SW provides flexibility and extensibility, the user of the open source software or library is responsible to ensure that the system is running the latest version of the source code in order to have the right level of security [42].

Openness in IoT is not just limited to open standards, open API's, open data, open processes, open operating system and open source code. Openness is also evident in architectural aspects of designing IoT systems. Vogel et al. [4] have described suitability of open IoT architecture approach for dynamic and heterogeneous IoT systems where the main characteristics are Flexibility, Customizability and Extensibility. Privacy and security issues in IoT requires high degree of flexibility as emphasized by Sicari et al. [39]. Miorandi et al. have also emphasized on the extensibility characteristic of open IoT systems [32]. They suggest to apply open architecture model during system and architecture design phase in order to guide the design and development aspects of open IoT system. It is emphasized to use open approaches over standardization which is hardly followed in IoT domain [4].

5 Empirical Study

This chapter presents the empirical results obtained from conducting interviews with the experts and practitioners from IoT industry. The results are related to properties of smart thing, properties of IoT system and constraints in IoT system. Also described are various security trends & challenges and security considerations. It also presents openness trend that is prevalent in IoT industry from practitioner's point of view. Transcriptions of the interview recordings are available in Appendix A: Interview of SM1-Appendix F: Interview of HX1.

5.1 Development of Interview Questions

There is a need to bridge the gap between theoretical research model and empirical study. In this section, formulated research questions and theoretical understanding will be used to develop an interview guide with various questions. Interview questions are designed according to the findings from semi-systematic literature study. This helps in reducing the gap between semi-systematic literature study and empirical findings. Following questions will be used during our qualitative interviews conducted as described in chapter 3.3.2.

Table 12 Interview Guide

#	***Question***	**Description**
1	*What is your job role in your organization?*	In order to facilitate good communication, this question will be used as an ice-breaker. Interviewer will get an opportunity to understand the persona of the interviewee, what kind of activities they perform in their organization. This question will help in ensuring interviewees awareness of the topic of study.
2	*What does IoT means to you?*	This question gives freedom to the interviewee to reflect over IoT in general and as well gives opportunity to make them aware of the domain in general.
3	*What are the properties associated with smart Things?*	This question helps us understand the definition of smart things from industry point of view.
4	*Are you aware of any general*	The intention of this question is to understand

	constraints in IoT?	interviewee's further awareness about IoT.
5	*How openness does affects IoT (Flexibility, Customizability, and Extensibility)?*	The intention of this question is to get interviewees opinion on usage of openness in IoT and other open methods and techniques.
6	*What are your views on security of Internet of Things?*	The intention of this question is to understand interviewee's awareness about security issues that exists in IoT domain. Since awareness is the key enabler in implementing security, it is very important to get practical views of the experts working in this domain.
7	*What are your views on privacy of Internet of Things?*	The intention of this question is to understand interviewee's awareness about privacy issues that exists in IoT domain. Since awareness is the key enabler in implementing privacy, it is very important to get practical views of the experts working in this domain.
8	*Why do you think considering security & privacy while designing IoT solutions is critical?*	This question helps in validating the purpose of the field in study. By getting interviewees view on motivation to implement security on IoT, we can gather a lot of useful information from industry point of view along with already gathered academic views. This question should also partially address inputs for Research Question#2.
9	*What are the challenges and constraints in using existing security measures on Internet of Things?*	The intention of this question is to fill gap between semi-systematic literature study and empirical study when it comes to Research Question#1.
10	*Are you aware of any existing security mechanisms within your organization that can address challenges in Internet of Things? What measures can you suggest?*	This question will partially address Research Question#2. This question provides an opportunity for brainstorming new ways of handling security & privacy in Internet of Things.
11	*Do you want to make any last statement for IoT community and developers?*	This question will help in getting practitioners most important issue or challenge or suggestion or view point within IoT domain. This could potentially generate data for Research Question#2.

There might be little variations in the questions asked to the interviewees based on their role within their organization. Also, the sequence of the questions may vary depending on the conversation during interviews.

5.2 Coding of Interview Questions

The questions enlisted in Table 13 will be used to interview experts and practitioners in the domain of IoT in order to get data regarding previously stated research questions. Q1, Q2, Q3 and Q4 will be used to get data regarding general awareness of the interviewee regarding IoT and its security & privacy implications. Q6, Q7, Q8 and Q9 will be used to gather data regarding RQ#1 and Q5, Q10 and Q11 will be used to gather data related to RQ#2.

Table 13 Coding of Interview Questions

<table>
<tr><th></th><th>IoT and Security Awareness</th><th>Security Trends & challenges (RQ1)</th><th>Implementing Open Secure IoT System (RQ2)</th></tr>
<tr><td rowspan="4">Questions</td><td>Q1. What is your job role in your organization?</td><td>Q6. What are your views on security of Internet of Things?</td><td>Q5. How Flexibility, Customizability, and Extensibility affects Internet of Things?</td></tr>
<tr><td>Q2. What does Internet of Things means to you?</td><td>Q7. What are your views on privacy of Internet of Things?</td><td rowspan="3">Q10. Are you aware of any existing security mechanisms within your organization that can address challenges in Internet of Things? What measures can you suggest?</td></tr>
<tr><td>Q3. What are the properties associated with smart Things?</td><td>Q8. Why do you think considering security & privacy while designing IoT solutions is critical?</td></tr>
<tr><td>Q4. Are you aware of any general constraints in Internet of Things?</td><td>Q9. What are the challenges or constraints in using existing security measures on Internet of Things?</td></tr>
<tr><td colspan="3"></td><td>Q11. Do you want to make any last statement for IoT community and developers?</td></tr>
</table>

5.3 Introduction to Interviewees

This section is used to give introduction to the interviewees. Respondent id, role, organization and how respondent is related to the field of study is the main information provided in this section.

Interviewee SM1 is a security architect at Security Department within Sony Mobile Communications AB. He relates himself to IoT Security & Privacy through security protocols and security software that he and his team develops. The interview with SM1 is available in Appendix A. *Interviewee SM2* is a security architect at Research & Incubation Department within Sony Mobile Communications AB. He works specifically with research and standardization parts. He is a security specialist for IoT projects. He looks at emerging technologies and applications within security and IoT. The interview with SM2 is available in Appendix B. *Interviewee TS1* is a technology leader at TechSource AB. He relates himself to IoT Security & Privacy through his technical expertise within Industry automation software that he and his team develops. He is the key decision maker when it comes to both technology and business. The interview with TS1 is available in Appendix C. *Interviewee SN1* is a technology expert at Sensative AB. He relates himself to IoT Security & Privacy through his technical expertise within home security products and software that he and his team develops. He is the key decision maker when it comes to technology and product deliveries. The interview with SN1 is available in Appendix D. *Interviewee AX1* is a security coach at Axis AB. He relates himself to IoT Security & Privacy through his security expertise within home surveillance software development process and products. He is the key decision maker for implementing security processes and software within his organization. The interview with AX1 is available in Appendix E. *Interviewee HS1* is a security expert at Hyker Security AB. He relates himself to IoT Security & Privacy through his security expertise within data security solutions that his company generates. He is the key decision maker for implementing security processes and software within his organization. The interview with HS1 is available in Appendix F.

5.4 Interview Results

The semi-structured interviews that was conducted with IoT practitioners enlisted in section 5.3 resulted in interesting results and will be summarized in this chapter. The empirical results gathered from qualitative interviews are categorized into IoT properties and constraints (section 5.4.1), security trends & challenges prevalent in IoT industry (section 5.4.2), various security & privacy considerations that IoT practitioners should follow (section 5.4.3), openness trend in IoT (section 5.4.4) and practitioners viewpoint on implementing open secure IoT system (section 5.4.5).

5.4.1 IoT Properties and Constraints

The term "IoT" is very versatile term covering various aspects of the connected things eco-system and has different meaning for different respondents depending on the organization they belong to. They have used terms such as "fancy", "buzzword", "strange", "nothing new" and "doesn't mean anything" etc. while describing what IoT means to them. According to SM1, IoT is a set of autonomous machines or things that can do certain assigned task and report the results. For this respondent, there is no IoT without internet. However, HS1 realizes IoT without internet as long as there is connectivity between things or applications. For this respondent, IoT is about connected things. For SM2, IoT is "Internet of anything". SN1 further elaborates that IoT is about creating world of connected things that can be used by lots of people and services both in private and public setup. AX1 brings a new perspective to IoT by defining it as a "software" packaged in a product that connects to the internet. The "software" is part of every component of the IoT eco-system. For this respondent essential elements of IoT eco-system are IoT thing, connection or internet and the backend (mostly cloud). Respondent HS1 states that, "IoT is about connecting machine to machine, but it's also about connecting machine to machine to humans and doing applications on that".

According to SM1 and SM2, smart thing is not just sensors which are just a data measurement points. It could be an Android device, actuators, etc. SM2 points out that some of the IoT things doesn't inherently has internet connectivity and relies on another device or gateway. Also, some IoT things does not have core embedded components and

relies mostly on cloud solution. TS1, uses the term "tool" for smart things which is used for human value driven applications. HS1 brings in the application perspective to IoT. For this respondent IoT thing is nothing but an application that solves user problems. SN1 and TS1 highlights connectivity and autonomy as the main properties of IoT. The properties or key features of IoT and smart things as pointed out by various respondents are available in below Table 14

Table 14 Key Properties & Features of IoT

Respondents	**Key Properties and Features of IoT**
SM1, SM2	It can **interact** with environment
SM1	It can perform **computation**
SM1	It can **react** on some data, e.g. trigger
SM1, AX1	It can perform its tasks **autonomously**, if needed.
SM1, SM2, TS1, SN1, AX1	It can **communicate** with other parts of the IoT eco-system, e.g. report collected data, etc.
SM1, SM2	It should be locatable and **addressable** in order to enable communication.
SM1, SM2	It can be **uniquely identified** based on the context or user privacy needs.
SM2	It can have distributed smartness
TS1	It should be capable of perform **data analysis** in the backend.

Apart from the above listed properties most of the respondents also highlighted heterogeneity, openness, flexibility and user centricity aspect of IoT systems. All the respondents emphasized security and privacy-preserving as the fundamental and mandatory property of any IoT system.

Respondents also highlighted various constraints in IoT system, which is described in the below Table 15. Respondent AX1, has not encountered any constraints in their IoT business since they use very powerful hardware for their camera's and have a constraint free cloud solution in the backend. This helps them choose powerful cipher suites for implementing security. This means that they have to deal with existing problems in security domain rather than investing time and resources in solving new problems of constrained IoT devices. Respondent HS1 suggests to take a practical approach in

tackling the problem of constrained computation power, battery power or memory. This respondent suggests to make end points less intelligent and move the resource consuming operations to hub or router etc. Respondent SN1 suggests middleware as a solution to address problem of fragmentation within IoT.

Table 15 Key Constraints in IoT

Respondents	Key Constraints of IoT
TS1, SN1	**Interoperability** related to protocol is not solvable at this stage. It's also about being able to connect multiple services to same services as pointed out by SN1.
SM1, TS1, SN1, SM2	**Fragmentation** is evident since players within IoT domain try to solve the existing problems of IoT in their own ways. Fragmentation also exits in terms of what technology is used to implement communication. There is lack of standardization. According to TS1, fragmentation is also introduced by the vendors and tool chain providers.
SM1, SM2, HS1	**Computational Power**, **Memory** and **Battery Power**. Battery power puts a limit on how much computation can be done by an IoT device. Low power devices usually have weak security implementations.
SM1	**Space** is also a limitation since IoT sensors are usually small. Some are small enough that they could be injected in human body. All needed technology should fit within the small sensor.
SM2, SM1	**Cost of technology** can be a constraint in low cost IoT device scenario. SM1 gives an example of expensive IoT devices being able to work with IPv6.
SN1	**Use of vertical model** instead of horizontal model for IoT solutions. Vertical solutions leads to interoperability problems. The solution to this problem is to move to horizontal model.

5.4.2 Security Trends & Challenges

Security understanding varies between individuals but all of them agree that security is mandatory and needs to be addressed as early in the development phase as possible. Without security & privacy IoT cannot work, says respondent TS1. All of them agree that

security cannot be implemented once product is shipped to the customer hence it has to be built into the product.

"The only security worth anything is the one that's being used or the only security worth anything is the one that you never even notice", says respondent HS1. Hence, people accept security or use security when it is hidden or built into the DNA of the product. Respondent SM1 suggests IoT users not to buy any IoT device that is not tested properly by a 3rd party company with security professionals.

For both respondent SM1 and HS1, security is about protection of generated sensitive data or information or assets by means of appropriate encryption technique and having full control over it. For respondent TS1, security should be enabled once the development project moves from prototyping phase to delivery phase. For this respondent Security is the key for IoT. For respondent AX1, it is not technology that makes IoT secure but it's the development community, process and tools. Also, IoT security is not about picking the right algorithm but it is about writing secure software with a good quality.

The property of security bug is that it is not a random event, there is an active attacker with an intent to exploit the bug, says respondent AX1. This respondent also emphasizes that there are usually a lot of security bug in the software. The actual problem is not to find them individually but finding enough of them in a reasonable and economical efforts. None of the respondents went into details of IoT related security attacks but they mentioned DOS, DDOS, message/data modification and/or alteration in their responses. 4 respondents highlighted that constrained nature of IoT devices puts restrictions on the type of security solutions that can be implemented.

Openness in IoT, i.e. use of open source and open components is an emerging trend as discussed by all the respondents. But what worries AX1, is that IoT players are using more open source components from smaller communities which are weaker in security and opens up attack surface.

A major trend that is observed in IoT domain right now is that **everything is moving towards public networks**, basically for cost reasons and hence, everything is exposed all of a sudden to malicious hands. Hence, respondent AX1, suggest IoT practitioners to take larger responsibility of securing our customers because not everybody can secure

themselves. This respondent says it is very important to get protected from the public network.

Another trend as highlighted by respondent HS1 is that **data generated by IoT** end points has a very large commercial value as soon as it is made available in the public network. Hence, lots of data based applications, data based analytics, and commercial data providers are visible. Hence, the data has to be locked down from start, opened up in real time and it must be possible to trade it and charge for it per data element.

Another trend is with usage of **blockchain** like technologies which are created for trust management and authentication. They can be used within IoT, says respondent SN1. However, it need modification e.g. by removing the problem of mining, adds respondent HS1. For respondent SM2, how secure blockchain really are, remains an open question. For respondent HS1, blockchain provides integrity of data and accessibility only but for confidentiality of data, an extra security mechanism need to be added to blockchain.

Many of the currently connected things were **not originally created to be connected** to internet and hence it is challenging to address software security in these products, says SM1 and TS1. SN1 further adds that internet from start was not built for security and it's hard to say if internet is the right technology for IoT or we have to start all over again.

According to respondent SN1, IoT community right now is putting way **too much focus on compatibility** between technology standards which is possible to overcome and way too little effort into figuring out how to make horizontal IoT models instead of the verticals. There are very little or poor attempts made when it comes to **standardization of security** processes says respondent AX1. The currently available standards for security processes, e.g. ISO27000 are made for IT environment and are really bad for IoT security. There might be increased regulatory requirements on IoT systems due to recent security attacks on governmental agencies, says respondent SM2.

The empirical results obtained related to several security challenges that exists within IoT are described below:

Growing number of devices and growing number of IoT supplier is a likely challenge according to respondent SN1. **Fragmentation** imposes further challenges on security due to differences in protocols used by different vendors. "Protocols built on top

of TCP/IP at Google level is quite different from challenges addressed by Ericsson/Verizon.", says respondent SM2. **Compatibility and interoperability** among fragmented protocols and technologies is a challenge according to respondent SN1. Complexity and multitude of standards makes existing security & privacy tools and mechanism to be in-sufficient says respondent HS1. **Standardization** is another challenge due to multiple verticals in IoT, each having their own limitations says respondent SM2. For example requirement of medical vertical might vary completely from industrial vertical.

There exists various security challenges that are **related to constrained resources** as highlighted by half of the respondents, i.e. SM1, SM2 and TS1. Established techniques such as TLS handshake and key sharing is an extreme overhead, says respondent SM2. Low cost hardware usually does not have capabilities to run public key and elliptic curve cryptography. Both respondents, SM1 and AX1 says that the traditional manufacturers of IoT things are least competent in software development and worse in developing secure software due to **lack of expertise** to handle secure software. This creates a big threat of introducing lots of security bugs into their products. Even IoT users have lack of security awareness and expertise. Hence, in order to handle security in such an **operational environment**, IoT practitioners should build security applications that can handle security for any kind of IoT users as recommended by respondent HS1.

According to respondent TS1, battery constraint plays an important role in providing **software upgrade**. Software could be upgraded over the air or manually. Respondent TS1 argues that sometimes it's cheaper to replace the device containing new SW and configurations than to create and maintain software upgrade mechanism. This respondent further adds that sometime operational environment makes it impossible to deploy software upgrade or affects the frequency of software upgrade. Cost is another factor affecting possibilities for software upgrade. Respondent SN1 highlights the challenge of **securing user integrity** at the same time opening up the IoT system. It's a challenge to implement **end-to-end security** in a horizontal model of IoT which contains IoT things, gateways, middleware, and cloud, says respondent SN1. One has to pay huge **penalties** to

the B2B customers, in case if security is breached in an industrial IoT. Hence, higher level of security should be ensured, says respondent TS1.

5.4.3 Security & Privacy Considerations for Secure IoT System

Considering the latest security trends & challenges within IoT, the practitioners should take into account various security considerations during development and deployment of secure IoT systems. These have been highlighted or suggested by different respondents which are as described below.

It is very important to have security requirements on IoT systems from **start of development activity** says both respondents SM1 and TS1. Security cannot be added once product is shipped to the customer says respondent TS1. Respondent SN1 further says that we have to build IoT architecture for security. We have to start with a system that is fundamentally secure, adds respondent HS1. Respondent AX1, also suggests **code review** as a technique to improve code quality.

Respondent AX1, has suggested to do a **risk assessment** on system level by use of tools like **threat modelling** etc. Identify components with high security risk within all the IoT software. And based on the results of security risk assessment, introduce security on the identified teams. Once the threats are identified in respective components, **introduce countermeasures** needed to handle that specific security threat in that specific context. Hence, respondent AX1, is emphasizing on implementing **context-aware security** rather than one-solution fits-all method.

It is important to consider if it is necessary for all the end point sensors to be capable to connect to public internet? According to both the respondent HS1 and SN1, instead of making stupid sensors to be the end points, an intelligent hub or gateway should be realized as the end point in IoT systems. This will help in mitigating the technological constraints.

Trust Management, should be in place in IoT systems as pointed out by respondents SM1, SM2 and SN1. Like in internet, it's partly about trust, partly about legal agreements with service providers and partly about knowing what data to share says respondent SN1. According to SN1, involvement of people in IoT system makes it complex to establish trust with multiple devices in the eco-system. Respondent SM2 suggests that

authorization of user or things is needed on case-to-case basis. This respondent further suggests usage of distributed ledger technologies to handle trust management within IoT systems.

Privacy is all about respect and is another term for confidentiality and ownership, says respondent HS1. Privacy is super important for respondent AX1 and they are building privacy measures into their secure development model. Both respondents SM1 and AX1, considers privacy as just one aspect of security and as a **subset of security**. They further claim that "**there is no privacy without security"** which is also supported by respondent HS1. If privacy is important in IoT systems then security needs to be implemented everywhere in the eco-system as recommended by respondent SM1. Respondent SN1, suggested to consider **data-privacy** so that the sensor generated data won't go to 3rd party if not desired. This respondent also mentions to consider **GDPR** requirements. According to respondent HS1, some IoT industry clients are skeptical about data-privacy on the cloud and prefers in-house solutions. There also exists privacy-issues in the systems where users are machines and not humans according to respondent HS1 since it might be possible to backtrack the actual human-user behind the machine-generated data.

Respondent SN1, suggests to identify the type of data and accordingly decide the privacy needs on it. This respondent highlights the importance of protecting the **integrity of the data**, i.e. if the data is correct and is not altered by anyone. One should do a cost benefit analysis to see what's the value of their data and what kind of risk budget can they have on their data within an organization or as a person. Accordingly, deploy appropriate **data security** mechanism says respondent HS1. This respondent further adds that it is easy to lock down everything and provide openness only when allowed. Both respondents SM1 and HS1 says if the data can be potentially used for commercial purpose it is important to **protect privacy of the data** before sharing it further. Respondent TS1 also suggests to **encrypt the data** originating from sensor. For sensitive data, respondent SN1 suggests to use techniques that can **securely erase data**. Respondent HS1 advocates use of **end-to-end** security in order to protect the valuable data.

Respondents SM1 and HS1, highlights use of **hardware security modules** over software security implementations in order to have better security on IoT device, e.g. integrated SIM cards, secure elements, secure enclave, ARM TrustZone, etc. TS1 advocates that such high security implementations are only needed in defense level applications. However, choice between the two might be driven based on the extra cost needed to have hardware security module, says TS1.

Scalability of security based on what kind of data is handled within the eco-system is an important aspect to consider according to respondent SN1. **Security Audits, certifications and approval process** should be considered in order to avoid huge penalties in case of a security breach according to respondent TS1. Certification also ensures delivering right quality product says respondent HS1.

Last but not the least, **security upgrades** has been identified as a major security consideration by half of the respondents, the others have mentioned it indirectly. According to respondent HS1, software upgrade is essential in how we develop secure software. It is a continuous process of patching security bugs all the time. Timely upgrade of software with available security patches has been ignored even by big players in IoT segment, says respondent SM1.

5.4.4 Openness in IoT

Openness for respondent TS1 is for IoT application to get the user trends and base its decisions or activities according to the trends. IoT players that sell their solutions via partners and those partners often adds new functionality to the existing products, hence Openness is very crucial for them, says respondent AX1. Openness is fundamental to IoT says respondent HS1 since one should be able to see the code, implement new functionality and test it in order to ensure security in code. Since openness allows sharing and interoperability rather than having patented or proprietary schemes, respondent SM2 really welcomes openness in IoT. Openness really helps the growth and maintenance of IoT systems says respondent SM1. Openness is mark of a good architecture says respondent SM2. Open systems also helps with speed of development and growth, hence, respondent TS1 encourages use of open solutions in IoT. One should start with completely open system and then think how to control openness. This argument is also

supported by respondent TS1 who suggests to lock down open systems on top depending on the target client.

Open source that is maintained by activity community is the most powerful thing according to respondent HS1. Respondent HS1 recommends usage of open source security libraries. Usage of open source code, e.g. openssl, etc., helps IoT player save enormous investment and creates cost benefits, says respondent AX1 and SM2. Respondent HS1, considers open source as a solution to innovation & invention and not a solution to everything. However, open source is not used as intended in IoT domains, e.g. critical security updates in kernel are ignored by not just small vendors but big players, says respondent SM1. Not properly maintained open source SW is prone to security bugs which are not patched in timely manner adds respondent HS1 and which is also supported by respondent TS1. Respondent AX1 argues that modern open sources projects are less secure than software done by commercial companies since it takes lots of investment to create secure software that cannot be done as hobby project. However, few selected open source projects are very secure and maintained. If an open source project is reasonably maintained or has confined use case then respondent AX1 suggests IoT community should not fork out.

Open operating system choice depends very much on the technical capabilities of IoT devices that e.g. Linux or Linux like etc. This fact has been acknowledged by both respondent SM1 and SM2. **Open API's** enables anyone to create services based on them, says respondent SN1 and allows other to use those services for their benefits. **Open data** will only be open as long as you can protect the commerciality of data says respondent HS1. **Open standards** helps in creating generic ways to solve standard tasks or goals says respondent SM1. Standardization is completely missing in IoT says respondent SN1. Respondent SM2 suggest that the standards should be more security focused.

Maintainability and innovation are the main aspects of an open system apart from the existing characteristics like flexibility, customizability and extensibility. Security is completely ignored says respondent HS1. However, respondents SM1, SN1 and HS1, considers security as an important characteristics of open IoT systems. IoT players using open source components needs to put vetting mechanism in order to figure out if those

components are secure enough or not, says respondent AX1. Openness comes with a risk says respondent AX1 since it is not possible to invest a lot in formally verifying how secure an open source component is. Hence, one can observe how the component behaves and be ready to patch it when needed. Respondent SM1 also emphasizes very much on the importance of security upgrades in open IoT systems. According to this respondent, it doesn't matter if it is an open system or a closed one as long as they maintain the software and provides necessary and critical security fixes. IoT community will not prefer an open IoT system that has security holes, adds respondent TS1.

5.4.5 Designing Open Secure IoT System

IoT security is not a technical problem but a process problem says respondent AX1. There is a need to introduce security awareness among IoT software practitioners and giving them appropriate security training. If practitioners are focusing on technical security problem, then they are talking about the wrong problem, adds respondent AX1. Respondent SM1 says IoT security is not about implementing existing techniques or mechanisms but it is more about mindset. Respondent SN1 supports this argument by mentioning that security problems can occur from weak security in development tools. This is further acknowledged by respondent HS1. It's not possible to state general practices or guidelines for designing secure IoT system says respondent SM1. It is very much context or use-case based. This argument is also supported by respondent AX1 who suggest use of context-aware security mechanisms. This implies instead of providing security recipes upfront, it is suggested to work with the teams and learn the pattern that works for their use case.

According to respondent SN1 security is a critical thing and we have to start thinking about security from early phase of SW development. It cannot be provided as an add-on once product has been shipped. This argument is supported by all other respondents. Respondent SM1, says close everything that needs to be from beginning and then open only what is needed to be open. This mindset helps reduce security risk immediately.

Respondent SM1 suggests creating a product offering that customer wants and then look at the high level requirements. Respondent SN1 adds that practitioners should build a solution according to customer requirements. Once we have the product requirements,

next step is to build system architecture making sure security is considered all the way. Practitioners should do security risk assessment e.g. using threat modeling immediately after system architecture is available says three of the respondents, i.e. HS1, SN1 and AX1. Based on the results of risk analysis, practitioners needs to frame security requirements on the system and platform says respondent AX1. Respondent TS1 suggest that based on security requirements, choose the right hardware components and right hardware vendor. We need to find right balance between cost and security says respondent SM1. In practice, this process of creating secure IoT system is iterative says respondent SN1. Throughout this process, practitioners should consider general security considerations highlighted in section 5.4.3. Respondent TS1 also suggest to employ a security architect who follows the latest security trends in the industry. Respondent HS1 says that it is responsibility of security architect to implement security correctly and completely. In order to find security bugs spread across the product, IoT practitioner's needs security toolbox consisting of threat modeling, architectural review, code review, running automated security tests, etc. suggests respondent AX1.

It is convenient to look at success models and reiterate the process says respondent TS1 and AX1. Respondent AX1 adds that the IoT practitioners should not try to reinvent the wheel because the problems they are encountering were applicable to other industry that exists and are mature now. Android security provides enough insight into how systems are built from security perspective. Hence, respondent SN1 suggests use of middleware as a solution to handle security. Security should be built into middleware apart from the underlying protocols according to respondent SN1. According to this respondent middleware solution will help IoT community develop services in a very easy manner that could be used by any IoT users. This middleware solution enables horizontal architecture of IoT which contains IoT things, gateways, middleware, and cloud, says respondent HS1. Respondent SM1 suggest use of tiny OS on small IoT things which can connect to bigger concentrators that can run rich OS. These can then connect to cloud which can do heavy operations of machine learning, etc. It is possible to add additional security layers but if the enabler layer is not secure then it is difficult to achieve true security, says respondent TS1.

6 Discussion

This chapter focuses on the discussion around the theoretical outcome from semi-systematic literature study and empirical outcome from applied research methods during the course of study. The research goal is analyzed considering the open secure IoT system which also served as the theme throughout the theoretical synthesis and empirical study.

6.1 Theoretical Findings

The main research goal of this thesis is to provide insights for IoT practitioners in order to improve security & privacy design for an open secure IoT system. Hence, the discussion around the semi-systematic literature study results is conducted with motivation to answer our research questions.

6.1.1 Revisiting Definition of IoT

The current state-of-the-art definitions for IoT (4.2.1) have touched upon several key properties of both smart thing and IoT (4.2.2 and 4.2.3). Some definitions are over simplified and some are overly complex [33]. However, none of those definitions provide a complete understanding of IoT considering security & privacy at the same time considering the original intentions of the term "IoT", as coined by Ashton [28].

Based on the original idea of Ashton, an attempt is made in order to contextualize the existing definition of IoT with security aspects,

"IoT is a network of interconnected identifiable things & software that are secured and enables them to interact with the world autonomously. It can communicate gathered information to other things or applications in a secure manner, thereby offering services to other people, other applications and other services."

This definition covers the various properties of smart things and IoT such as connectivity, communicability, identifiability, autonomy, interaction with environment, and most importantly security.

6.1.2 Trends & Challenges

Openness is one of the emerging trend that is evident in IoT domains (4.2.3 and 2.2). More and more IoT players are motivated to use open systems due to the associated benefits like easiness, convenience and fast development resulting in major cost-savings (2.2). Openness is about using open standards, open data, open API, open processes, open source, open OS and open architecture (2.2 and 4.6). Openness is not limited to extensibility, customizability and flexibility of the IoT systems but is extending to include security & privacy aspects (2.2).

Fast growth in IoT is a key trend and is evident from growing number of devices (1.1), growing number of domains ranging from personal wearables to smart cities and industries (2.1) and growing number of IoT players varying from traditional software companies to dedicated hardware manufacturers having least experience of software development. However, this fast growth has resulted in fragmentation and heterogeneity in the IoT industry (4.2.3, 4.2.4). It is also evident that these companies are trying to connect every physical object with public network or internet using sensor technology, Wi-Fi or modem. It is also seen that in constrained IoT systems, smart physical objects are interacting with each other and also with humans in a restricted operating environment. This **is not given enough importance** during analysis and design phase [7].

IoT systems are easy to hack due to heterogeneity, key constraints and growing number of nodes or devices (4.3). Hence, many security attacks are been recorded on IoT systems (4.3). These factors are motivating IoT players to consider security & privacy as an important aspect during software development life cycle (4.4). One of the main trend identified during semi-systematic literature study is that **IoT practitioners does not consider security & privacy as a big concern from start**, i.e. they try to apply security retroactively or as an add-on. The study conducted on existing literature highlights that in most cases focus is more on the implementation details and reuse of existing security & privacy mechanisms without considering special properties and features of IoT system (4.2.3). The mechanisms that exits currently to implement security & privacy on each of the mentioned IoT layers [7] are insufficient or inapplicable in their current state due to

the constraints that exists in IoT systems [32][7][39]. Hence, there exists need to adapt or customize existing security & privacy mechanisms for IoT systems.

Among various properties and characteristics of IoT systems as described in section 4.2.3, security and privacy-preserving mechanisms have been highlighted as the most important characteristics for any IoT systems by many researchers including [32] [39][40]. In order to have enhanced security & privacy in an IoT system, properties like flexibility, scalability, heterogeneity, autonomy, mobility and interoperability should be critically considered by the IoT practitioners. However, energy-optimized solutions, user centricity, self-organization capabilities, mobility, communicability, semantic interoperability and data management are some of the key features that IoT practitioners should consider in their implementations.

Based on the state-of-the-art within IoT security and privacy, the key challenges in using existing security & privacy measures on IoT can be classified into following categories (section 4.5) as described below.

Challenges related to resource constraints: These challenges arise due to lack of resources available on IoT devices and networks. Some of the challenges mentioned in this category can be addressed by reengineering existing mechanisms, e.g. crypto algorithm, security & privacy tools. Few challenges needs a rethinking from designing hardware itself and other challenges are even harder to address, e.g. lack of MMU, hardware root of trust, etc.

Challenges related to heterogeneity: These challenges arise due to variety in security & privacy solutions used. Many of these challenges can be addressed with usage of openness in IoT and standardization.

Challenges related to privacy: These challenges arise due to nature of data involved in IoT systems, dynamism, ubiquity and amount of data, replacement of users with things and other privacy related issues. Handling privacy in IoT calls for user centric development instead of technology centric development.

Challenges related to software upgrades: These challenges arise due to software upgrade of smart things and other elements within IoT systems. Based on the results of

semi-systematic literature study the software upgrade solutions and processes needs to be considered from early design or architectural phase.

Challenges related to operational environment: These challenges arise due to the environment in which smart things operates. Some of the challenges mentioned in this category can be addressed by simple reengineering, while others need thorough thinking throughout the software development life cycle.

6.1.3 Open Secure IoT System

Based on the trends that are seen in IoT system development and trends in addressing security issues in IoT as seen in chapter 6.1.2 and also the semi-systematic literature study (chapter 4), it is suggested that the focus should be shifted on openness of the IoT system in order to create a flexible, extensible and customizable IoT system. Open architecture approach was suggested in order to realize above openness characteristics (section 4.6). This openness can be achieved by use of following openness aspects, i.e. open standards, open API's, open data, open processes, open OS and open source code (section 4.6).

It is also seen that security of IoT system is essential and integral part of it (sections 2.1, 4.2.3, 4.3, 4.4). Security is not just needed but is mandatory for a successful deployment and execution of IoT system. Security needs to be built from start and cannot be implemented retroactively or in other words IoT systems should have security by design. Moreover, security cannot be neglected during any phase of IoT software development lifecycle. Privacy is a subset of security (5.4.3) and hence IoT systems should also have privacy by design.

As seen above, it is motivated to design an IoT system that is an open system and has security by design or in another words IoT industry needs to start thinking about **open secure IoT systems**. The key security & privacy considerations as shown in the results of section 4.4 should be considered from initial phase of open secure IoT system development. **Security** offers protection against threats & vulnerabilities, intrusions, unauthorized access and implements privacy protection mechanism (section 4.3, 4.4). Privacy cannot be implemented without security in place and hence privacy is considered as one of the properties of security characteristic of open secure IoT systems (section 4.4).

The IoT practitioners needs to consider following security aspects when designing open secure IoT system, i.e.

- **Contextual awareness** in order to achieve context based access control and context based security (section 4.4).
- **Cost-effectiveness** in order to make appropriate security choice e.g. hardware vs software security solutions, choosing the right security toolbox, etc. (section 4.4).
- **Heterogeneity** in security implementations needs to be handled when different smart things connects and communicates with each other in order to achieve interoperability (section 4.4).
- **Trust manageability** for device trust, entity trust and data trust and also strong authenticity in order to prevent unauthorized smart things and humans to access IoT devices and systems (section 4.4).
- **Privacy-preservability** in order to achieve confidentiality and integrity of data. Data privacy, i.e. protection of personal, sensitive and enterprise data includes operations like data authenticity, data aggregation, data anonymity, data un-linkability and secure erase of data (section 4.4).
- **Software updatability** has been identified as an important security consideration since there is no security if the software is not continuously patched with security fixes (section 4.5).
- **Standardization** is needed in order to handle fragmentation visible in IoT industry (section 4.4).
- **Digital divide** should be handled since there exists differences in level of understanding of security & privacy risks among IoT users (section 4.4).

These security and openness aspects obtained from theoretical findings can be visualized into a model for designing open secure IoT system presented in Figure 6. This system has two major characteristics, i.e. openness and security represented with big rectangular boxes followed by various design aspects represented by smaller boxes. When designing an IoT system based on openness and security, their respective aspects needs to be considered by the IoT practitioners.

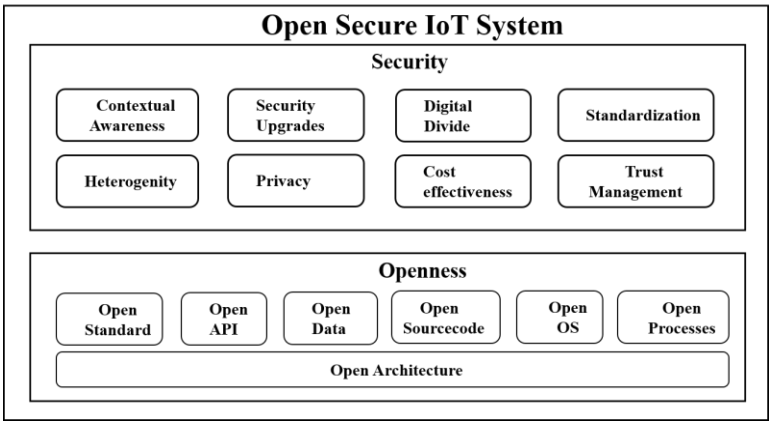

Figure 6 Open Secure IoT System – Theoretical perspective

6.2 Empirical Findings

The discussion around the interview results is conducted with motivation to answer our research questions and validate results obtained from semi-systematic literature study (chapter 4). The definition provided in section 6.1.1 is in-line with understanding of IoT among IoT practitioners as described in section 5.4.1

6.2.1 Trends & Challenges

Several trends & challenges has been highlighted by experts from IoT industry in their interview results.

Openness in IoT is seen as an emerging trend in IoT systems depicted with usage of open source components, open API, open standards, open data (section 5.4.2). However, improper choice of open source leads to opening up larger attack surface. Such a trend is prominent since openness allows sharing and interoperability, helps growth and maintainability, increases speed of development and reduces cost of development (5.4.4). Openness trend is also highlighted in details in the conducted semi-systematic literature study (chapter 4).

From both semi-systematic literature study and empirical results it is obvious that there exists a trend **to connect all the physical object to internet or public network**. This has resulted in fast growth of IoT at the same time exposes every physical object that is personal or sensitive in nature to malicious hands (Section 5.4.2, 6.1.2). Hence, it is crucial to implement necessary security & privacy preserving mechanism in IoT.

However, most of the IoT devices and many technologies seen in today's IoT world were **not originally created with an intention to be connected to internet**, i.e. exposed to public network. Although, it is creating ample amount of services and applications that will benefit human life, however it is creating opportunities for target security attacks (Section 5.4.2 and 4.3).

Another trend that is evident in IoT is about **wide sharing of data** generated by IoT end points (Section 5.4.2). This trend was not highlighted in the selected papers for semi-systematic literature study. However, both semi-systematic literature study and empirical evidences points to the fact that data sharing has resulted in data security, data privacy and end-to-end security related requirements. This data also has huge commercial value hence, it should be possible to trade data and lock it down as soon as it is generated.

When it comes to trust management and authentication, **blockchain related technologies** are emerging at a fast pace. Such techniques provide integrity and easy accessibility of data when needed. It also helps in practical implementation of data-sharing (Section 5.4.2). Another trend that is evident is that IoT players are creating **vertical solutions** resulting in fragmentation in IoT industry. Horizontal model that consists mainly of a middleware kind of solution help address issues related to interoperability, heterogeneity and fragmentation (Section 5.4.2).

As seen from semi-systematic literature study there exists various categories of security & privacy related challenges within IoT. Empirical evidences also supports similar categories of challenges.

Challenges related to resource constraints (section 4.5): These challenges are related to processing power, battery power, memory constraints, space constraints, etc. (Appendix A: Interview of SM1). In a resource constrained environment, it is difficult or impossible to use stronger cipher suites, best security algorithms, etc. (Appendix E: Interview of AX1).

Challenges related to heterogeneity (section 4.5). Next category of challenges occur due to fragmentation of protocols used by different vendors (Section 5.4.2). Hence compatibility and interoperability is a big challenge. Complexity and multitude of standards used for enabler technologies makes existing security & privacy tools and

mechanism to be in-sufficient (Section 5.4.2). Lack of standardization is evident in IoT domain (Section 5.4.2).

Challenges related to privacy (section 4.5). Heterogeneity in usage of security & privacy preserving mechanisms imposes challenge on privacy of data and IoT systems (Section 5.4.2). There exists challenges in securing user integrity at the same time opening up the IoT system (Section 5.4.2). One has to pay huge **penalties** to the B2B customers, in case if privacy & security is compromised in an industrial IoT setup (Section 5.4.2).

Challenges related to software upgrades (section 4.5). Battery constraint plays an important role in providing software upgrade (section 5.4.2). Sometimes even operational environment makes it impossible to deploy software upgrade or affects the frequency of software upgrade (Section 5.4.2). Cost plays a major role in providing software upgrade since it might be expensive to create and maintain software upgrade mechanisms (Section 5.4.2).

Challenges related to operational environment (section 4.5). Final category of challenges are imposed by operational environment in which IoT devices run. Growing number of devices and increased attack surface (Section 5.4.2, 4.3) pose various security challenges. Growing number of IoT supplier is also another challenge since it creates fragmentation, vertical thinking, etc. It is evident that there is lack of expertise to handle secure software and traditional manufactures of IoT things are least competent in software development and worse in developing secure software (Section 5.4.2). All these challenges impose great security threats. Even IoT users have lack of security awareness & expertise and this creates digital-divide issue. It is a challenge to implement end-to-end security in a horizontal model of IoT which contains IoT things, gateways, middleware, and cloud (Section 5.4.2).

6.2.2 Open Secure IoT System

We have already seen in section 6.1.3 that there is an openness trend in IoT domain which is also supported by empirical evidences presented in section 5.4.4. It is fundamental and crucial to have openness in IoT since it allows interoperability and sharing of source code, data, api and other artefacts. Openness helps the growth,

maintenance and speed of development. It is also suggested to start with completely open system and then take appropriate decisions to control openness as desired. Empirical results shows that ways to introduce openness in IoT system is by using following aspects, i.e. open source code, open OS, Open API's, open data and open standards. Openness brings innovation in the system.

Security is a mandatory characteristic for IoT systems and needs to be addressed as early in the IoT development lifecycle since it cannot be pushed once product is shipped (section 5.4.2, 6.1.3). Security is the key enabler for IoT (section 5.4.2). There are enough evidences from both theoretical findings and empirical data to support security as a key design aspect (section 6.1, 6.2). However, security is usually ignored in such an open IoT system. Hence, the IoT practitioner's should consider following security aspects when designing open secure IoT system, i.e.

- Security problem is not a tool or implementation issue, however, it is more of a **people and process** issue (section 5.4.5). It is not technology that makes IoT secure but it's the development community, process and tools that are followed which makes things secure.
- Security starts with **awareness** and right mindset. Hence, security cannot be introduced after the product has been shipped but needs to be integrated in all phase of the IoT system development lifecycle. (section 5.4.5).
- **Cost effectiveness** of security solution is needed since it plays an important role in making security choice, e.g. platform or vendor selection, harware vs software security, etc. (section 5.4)
- It is not possible to state general practices or guidelines for designing secure IoT systems. However, IoT security practitioners needs to consider **context aware** security where they work with the respective software team to understand their specific context or use case and learn security pattern that works for that particular team. (section 5.4.3, 5.4.5).
- Performing security **risk assesment** using appropriate tools like threat modelling, system architecture review, etc. helps security practitioners frame appropriate security requirements on the systems. (section 5.4.3, 5.4.5).

- IoT practitioners should create their **security toolbox** consisting of threat modeling, architectural review, code review, running automated security tests, etc. in order to find security bugs and fix them to ensure right quality (section 5.4.5). IoT security is not only about picking the right algorithm but it is mostly about writing secure software with a good quality.
- **Security Audits, certifications and approval process** should be considered in order to avoid huge penalties in case of a security breach. It also ensures delivering right quality product. (Section 5.4.3).
- **Security upgrade** is a major security consideration. It is a continuos process and hence it is very important to provide timely security upgrades. (Section 5.4.3).
- It is very important to choose as strong **algorithms** and cipher suites as possible considering various constraints that exists in the system. Such a choice enables best possible security solution. (section 5.4.1).
- **Trust management** needs to be considered since user trust is not just about people-people or people-machine but is also about machine-machine. Hence, appopriate authentication and authorization mechanisms needs to be in place. (Section 5.4.3).
- **Privacy** is utmost important aspect of IoT and needs to be preserved absolutely. It is not just about confidentiality and ownership of data but also about respect. Hence, new GDPR regulations are evident these days. It is important to protect data-privacy, ensure integrity of data, confidentiality of data, secure erasing of data, etc. It is also suggested to use end-to-end security in order to protect valuable data generated in IoT. There is no privacy without security in place (section 5.4.3).

These security and openness aspects obtained from empirical findings can be visualized into a model for designing open secure IoT system presented in Figure 7. This system has two major characteristics, i.e. openness and security represented with big rectangular boxes followed by various design aspects represented by smaller boxes.

When designing an IoT system based on openness and security, their respective aspects needs to be considered by the IoT practitioners.

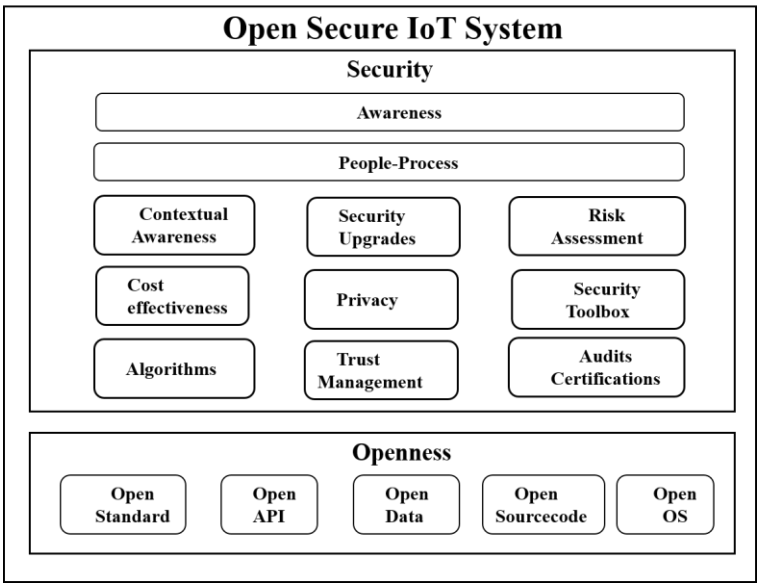

Figure 7 Open Secure IoT System – Empirical perspective

6.3 Designing Open Secure IoT System for Practitioners

So far we have seen theoretical model (6.1.3) and empirical model (6.2.2) that shows the design aspects that IoT practitioner should consider when implementing open secure IoT system. Here we present the consolidated results and insights for IoT practitioners in order to improve security & privacy design for an open secure IoT system.

As seen from sections 6.1 and 6.2 similar trends were encountered in both theoretical findings and empirical results, e.g. fast growth in IoT, wide usage of public network to connect everything and most importantly openness in IoT. However, few more trends like wide sharing of data, usage of blockchain technologies, connecting new hardware to public network even though it was not originally intended to, and lastly, creation of vertical solutions were only obtained from empirical findings.

We have also seen five categories of security & privacy related challenges that were obtained from semi-systematic literature study (section 4.5) which were validated using empirical findings (section 6.2.1). They are challenges related to constrained resources, challenges related to heterogeneity, challenges related to privacy, challenges related to software upgrades and challenges related to operational environment.

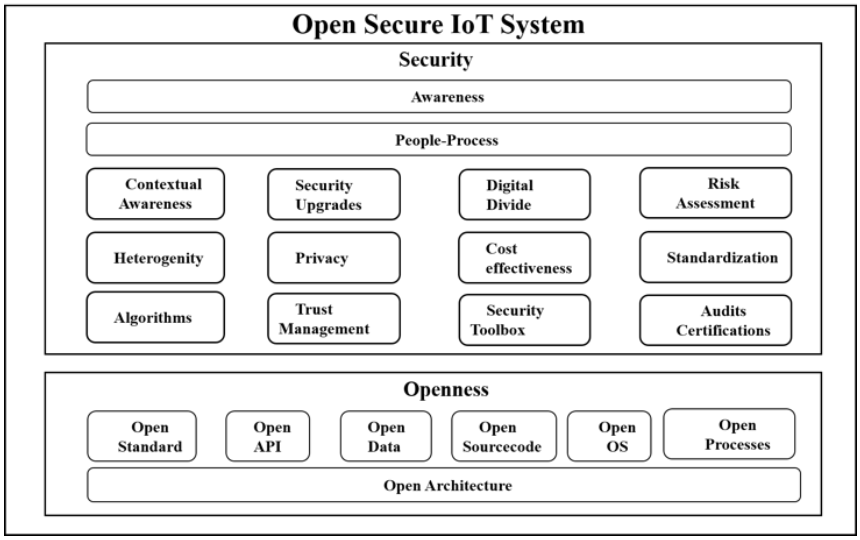

Figure 8 Open Secure IoT System – Proposed Model

In order to implement open secure IoT systems, IoT practitioners should consider following security aspects, i.e. Awareness (section 6.2.2), People and Process (section 6.2.2), Contextual awareness (section 6.1.3 and 6.2.2), Cost-effectiveness (section 6.1.3 and 6.2.2), Heterogeneity (section 6.1.3), Trust manageability (section 6.1.3 and 6.2.2), Privacy-preservability (section 6.1.3 and 6.2.2), Security upgrades (section 6.1.3 and 6.2.2), Standardization (section 6.1.3), Digital divide (section 6.1.3), Risk assesment (section 6.2.2), Security toolbox (section 6.2.2), Security Audits, certifications and approval process (section 6.2.2) and Algorithms (section 6.2.2). They should also consider following openness aspects, i.e. open standard, open api, open data, open source code, open OS, open processes and open architecture.

Above mentioned aspects can be visualized into a model for designing open secure IoT system. This system has two major characteristics, i.e. openness and security. When designing an IoT system based on openness and security, their respective aspects needs to be considered by the IoT practitioners. Figure 8, shows the proposed model for designing open secure IoT system. Where two main characteristics, i.e. security and openness are represented with big rectangular boxes where each box consists of various design aspects to be considered represented by small rectangular boxes.

6.4 Limitations and Threats to Validity

Various limitations and threats were encountered during the research and analysis phase. Actual implementation of various proposed security considerations is out of scope of this study. Semi-systematic literature study was conducted by single researcher and hence there was no opportunity for peer review, etc. However, interview method was used to validate results obtained from semi-systematic literature study. Various inclusion and exclusion criteria were defined as explained in chapter 3.2.3 in order to handle encountered threats to validity. Search process and quality assessment criteria were defined in order to select high quality research material from valid and renowned sources.

As explained in 3.3.2.1, interviews were conducted only within southern part of Sweden. A total of 6 interviews were conducted which might be a small data set to generalize results. In addition, the results obtained from interviews are not validated with any practical implementations but can be considered for future work. Handling of researcher's bias during the interview is explained in details in chapter 3.3.4. In order to minimize bias, interviewees were selected from organizations ranging from start-ups to giant players in IoT industry. Moreover, interviewees were selected based on varying roles, i.e. security architects, senior architect, technology experts, technology leader, security coach, security expert, etc. in order to bring diversity in the collected data. The selected roles are relevant to the topic of research since they are the key security decision makers within their organization and follow latest security trends in IoT industry. Also, they deal with various security & privacy related challenges in their operations.

In this study, a model is proposed for IoT practitioners to consider when implementing open secure IoT system, however, due to time constraints it was not possible to create grouping, relationships or mapping between different designs aspects. Even the model does not shows the priority or importance of each aspect. However, these cannot be considered as obstacles in using the proposed model in practice since it is most important to consider the model as a whole and apply it according to the needs of respective organization.

7 Conclusion

A short discussion is presented to conclude with a summary and answering the research questions formulated in previous chapters. A thought has also been given on future prospective research opportunities within the field of IoT security & privacy.

7.1 Research Questions - Revisited

The main goal of the thesis was to provide insights for IoT practitioners in order to improve security & privacy design for an open secure IoT system, i.e. an IoT system that is open and consider security at its heart rather than handling security issues reactively (section 1.3). In addressing this goal, the body of knowledge was acquired by conducting semi-systematic literature study (chapter 4). The focus was on researches reported in primary journals and conferences related to IoT. The results obtained from semi-systematic literature study were validated by conducting qualitative interview method. Interviews were conducted with the experts and practitioners in IoT industry (chapter 5). In order to provide better insights into this research, Figure 9 provides an overview and justifies how the thesis evolved by providing mapped details that shows relationship between the theoretical findings, empirical findings and proposed model as outcome.

Two research questions were formulated in order to address goal of the thesis. RQ1 helped in understanding the trends & challenges in using existing security & privacy mechanisms within Internet of Things. RQ2 helped us figure out the design aspects that practitioners needs to consider when implementing open secure IoT systems.

The study has resulted in few key findings which are described below based on the work presented in previous chapters.

RQ1: *What are the trends & challenges in using existing security & privacy mechanisms within Internet of Things?*

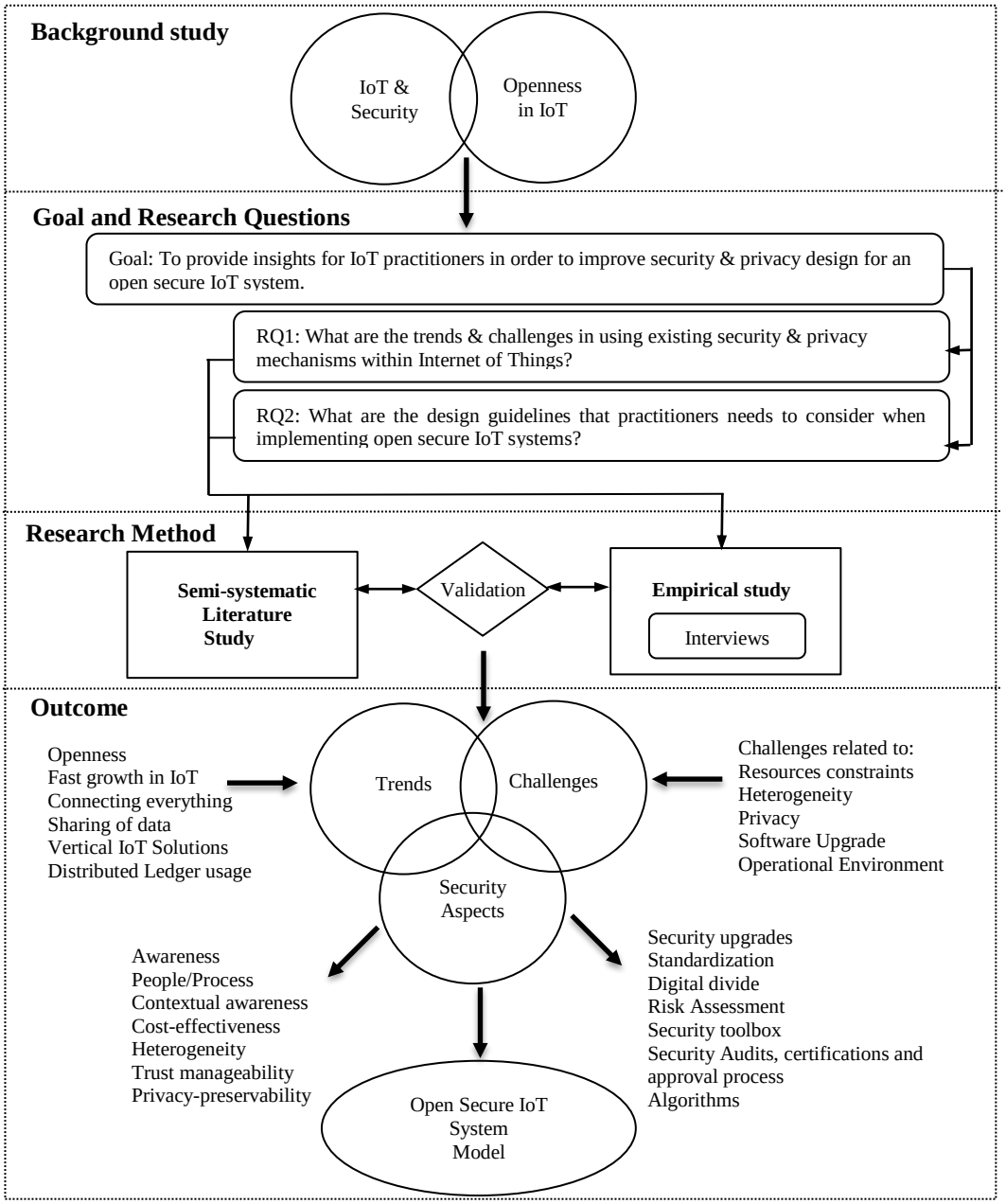

Figure 9 Thesis evolution w.r.t research question, method and outcome

Openness was observed as a major trend in IoT industry resulting in usage of open source, open data, open API, open standards, etc.

Other trends that are observed are as follows,

- Fast growth in IoT
- Connecting everything to public network or internet, sometimes, even when the hardware was not originally designed to be connected to internet

- Wide sharing of data generated from IoT sensors
- Creation of vertical IoT solutions
- Usage of blockchain like technologies

Security was highlighted as a mandatory and key characteristic of IoT system. The results shows that existing mechanisms to handle security & privacy in IoT is not sufficient. Their usage pose various challenges which can be broadly categorized into

- challenges related to resource constraints
- challenges related to heterogeneity
- challenges related to privacy
- challenges related to software upgrades
- challenges related to operational environment

RQ2: *What are the design aspects that practitioners needs to consider when implementing open secure IoT systems?*

The study resulted in an outcome that it is not possible to state general practices or guidelines for designing secure IoT systems. Security is not only a technical problem but more of an awareness, mindset, people or process issue. However, there are various security design aspects that needs to be considered by IoT practitioners when implementing open secure IoT systems. These design aspects are security awareness and mindset, people and process, contextual awareness, cost-effectiveness, heterogeneity, trust management, privacy-preservability, security upgrades, standardization, digital divide, risk assesment, security toolbox, security audits, certifications & approval process and finally efficient Algorithms.

7.2 Contributions

This thesis contributes to the field of IoT and security by proposing Open Secure IoT System design model (section 6.3). It provides design insights for IoT practitioners to implement an open secure IoT system (section 7.1). It also presents the latest trends & challenges related to security & privacy within IoT domain (section 7.1). Moreover, this thesis highlights the gap between the academic research and industry best practices.

Apart from above contributions, this thesis also provides an extended definition of IoT (section 6.1.1) based on the original idea of the term IoT at the same time considering the key security aspect of IoT.

7.3 Proposal For Further Studies

Future work that can be carried out as a follow up of this research study are following:

- An online survey with IoT users can be conducted in order to get general understanding of their usage and awareness regarding security and privacy
- The proposed model to implement open secure IoT system as described in section 6.3 can be applied on an industrial setup within a pilot project to validate the outcome of this study.
- Further work can be carried out by creating grouping, relationships or mapping between different designs aspects highlighted in the proposed model for Open Secure IoT Systems (section 6.3)

References

[1] Ericsson Mobility Report. Internet of Things forecast, 2017. Available: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast [Accessed: Sep. 5, 2017].
[2] IoT Security Foundation. 2017. Available: https://www.iotsecurityfoundation.org/about-us/. [Accessed: Apr. 9, 2017].
[3] J. Wallen. Five nightmarish attacks that show the risks of IoT security. 2017. Available: http://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/. [Accessed: Oct. 3, 2017].
[4] B. Vogel, D. Gkouskos. An Open Architecture Approach: Towards Common Design Principles for an IoT Architecture. 2017. pp. 1-4.
[5] B. Vogel, A. Kurti, T. Mikkonen, and M. Milrad. Towards an Open Architecture Model for Web and Mobile Software: Characteristics and Validity Properties. In Computer Software and Applications Conference (COMPSAC), 2014 IEEE 38th Annual. 2014. pp. 476–485.
[6] H. Petersen, E. Baccelli, and M. Wahlisch. Interoperable Services on Constrained Devices in the Internet of Things. 2014. pp. 1-3.
[7] E. Fernandes, A. Rahmati, K. Eykholt, A. Prakash. Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges? 2017. pp. 1-4.
[8] S. Boddy, J. Shattuck. Threat analysis report, The hunt for IOT. F5Labs. 2017. Available: https://f5.com/labs/articles/threat-intelligence/ddos/the-hunt-for-iot-the-rise-of-thingbots. [Accessed: Dec. 1, 2017].
[9] F. Shull, J. Singer, and D. I. K. Sjöberg, editors, Guide to Advanced Empirical Software Engineering. Springer London, 2008. pp. 337-364.
[10] M. Elkhodr, S. Shahrestani and H. Cheung. The Internet of things: New Interoperability, Management and Security Challenges. International Journal of Network Security & Its Applications (IJNSA) Vol.8, No.2, March 2016. pp. 2, 8-14.
[11] R. K. Yin. Case study research: design and methods. 3rd ed., Sage, Thousand Oaks. California. 2003.
[12] R. Neisse, G. Steri, I. N. Fovino, G. Baldini. A Model-based Security Toolkit for the Internet of Things. 2015. pp. 2-3.
[13] S. Easterbrook, J. Singer, M. Storey, and D. Damian. Selecting empirical methods for software engineering research, in F. Shull, J. Singer, and D. I. K. Sjberg, editors, Guide to Advanced Empirical Software Engineering, pp. 285-311. Springer London, 2008.
[14] M. Botterman, "Internet of Things: an early reality of the Future Internet," Workshop Report, European Commission Information Society and Media, May 2009.
[15] A. Bryman. Samhällsvetenskapliga metoder, 1:3, Malmö: Liber. 2006.
[16] J.W. Creswell. Qualitative Inquiry and Research Design: Choosing. Among Five Approaches. California, Sage. 2007. pp. 140-143, 239-240.
[17] D. M. Myers, & M. Newman. The qualitative interview in IS research: Examining the craft. Information and Organization. 2007. pp. 23-24.
[18] S. Kvale, & S. Brinkmann. InterViews: Learning the Craft of Qualitative Research Interviewing. London, Sage. 2009. pp. 97-183
[19] M. Q. Patton. Qualitative Evaluation and Research Methods. 2nd ed. Newbury Park, CA: Sage. 1990. pp. 341-348.
[20] C. Seale. The quality of qualitative research. Sage, London. 1999. pp. 30-50.
[21] D. Schlagwein, K. Conboy, J. Feller, et al. “Openness” with and without Information Technology: a framework and a brief history. Journal of Information Technology. 2017. pp 297–305.

[22] J. Buckley et al. “Towards a taxonomy of software change”. In: Journal of Software Maintenance and Evolution: Research and Practice 17.5. 2005. pp. 309–332.
[23] D. Oblinger. ”EDUCAUSE Values: Openness” January 2009. [Online]. Available: https://er.educause.edu/articles/2009/1/educause-values-openness [Accessed: May. 19, 2018].
[24] B. Kitchenham, Procedures for performing systematic reviews. 2004. pp. 1-27.
[25] F.A. Alaba et al. Internet of Things security: A survey. Journal of Network and Computer Applications. 2017. pp 10-28.
[26] B. Kitchenham, et al., Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software. April 2007. pp 571-583.
[27] T. Dyba, T. Dingsoyr, and G.K. Hanssen, “Applying Systematic Reviews to Diverse Study Types: An Experience Report,” Proc. Int’l Symp. Empirial Software Eng. and Measurement. 2007. pp. 225-234.
[28] K. Ashton. The Internet of Things Thing. RFID Journal. 2009. Available: http://www.rfidjournal.com/articles/view?4986. [Accessed: Mar. 11, 2018].
[29] P.P. Ray. A survey on Internet of Things architectures Journal of Computer and Information Sciences. 2016.
[30] IERC, “Internet of Things”. 2014. http://www.internet-of-things-research.eu/about_iot.htm [Accessed: Mar. 03, 2018].
[31] M. Ge, J. B. Hong, W. Guttmann, D. S. Kim. A framework for automating security analysis of the internet of things. Journal of Network and Computer Applications. 2017. pp 12-27.
[32] D. Miorandi, S. Sicari, F. D. Pellegrini, I. Chlamta. Internet of things: Vision, applications and research challenges. Journal of Ad Hoc Networks 10. 2012. pp 1497–1516.
[33] L.Atzori, A. Iera, G. Morabito. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Journal of Adhoc networks. 2017. pp 122-140.
[34] R. Roman, J. Zhou, J. Lopez. On the features and challenges of security & privacy in distributed internet of things. Journal of Computer Networks. 2013. pp 2266-2279.
[35] A. R. Sfar, E. Nataliziob, Y. Challalc, Z. Chtouroua. A roadmap for security challenges in the Internet of Things. Journal Digital Communications and Networks. April 2017. pp. 1-20.
[36] E. Bertino. Data Privacy for IoT Systems Concepts, Approaches, and Research Directions. IEEE International Conference on Big Data. 2016. pp 3645-3647.
[37] J. Gubbi, R. Buyyab, S. Marusic, M. Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. Journal of Future Generation Computer Systems. 2013. pp 1645-1660.
[38] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Computer. Network. 2010. pp 2787–2805.
[39] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015. pp 146-164.
[40] I. Butun. Privacy and Trust Relations in Internet of Things from the User Point of View. Computing and Communication Workshop and Conference (CCWC), IEEE 7th Annual. 2017. pp 1-5
[41] Z. Wang et al. Review on open source operating systems for internet of things. 2017. J. Phys.: Conf. Ser. 887 012044
[42] S. M. Devine. Open source and the Internet of Things. 2018. pp 14-19.
[43] Lite OS. Available: http://www.huawei.com/minisite/liteos/cn/ [Accessed: May. 11, 2018].
[44] Contiki. Available: http://www.contiki-os.org/ [Accessed: May. 11, 2018].
[45] MindSphere by Siemens. Available: https://siemens.mindsphere.io/ [Accessed: May. 11, 2018].
[46] RIOT. Available: http://www.riot-os.org/ [Accessed: May. 11, 2018].
[47] Brillo by Google. Available: https://developers.google.com/brillo/ [Accessed: May. 11, 2018].

[48] Mbed OS by ARM. Available: http://www.mbed.com/ [Accessed: May. 11, 2018].
[49] Tiny OS. Available: https://github.com/tinyos [Accessed: May. 11, 2018].
[50] Free RTOS. Available: http://www.freertos.org/ [Accessed: May. 11, 2018].
[51] UClinux. Available: http://www.uclinux.org/ [Accessed: May. 11, 2018].
[52] µC/OS. Available: https://www.micrium.com/rtos/ [Accessed: May. 11, 2018].

Appendix A: Interview of SM1

Researcher: What is your job role in your organization? How do you contribute to IoT?
SM1: My current role is lead engineer in SW sec team within Sony group. My contribution at this role is equal to 0. I can treat myself mostly as entrepreneur since I have my own company and several pet projects are within IoT sphere as I can see it. To be honest it is really broad. Definition that we can discuss what it means.
Researcher: That is the second question I have, i.e. what does Internet of Things means to you? So maybe you can merge answers to both question.
SM1: Definitely. Specially for me, because if you take a look at Wikipedia or any other encyclopedia that can provide some definition it can go in a slightly different direction but for me it's one or set of different machine, computers gadgets doesn't matter. This one is optional that can do some task without a human being, a person without any operator automatically, that's the main thing from my point of view. Because for example if you will speak about something or everything that can be connected to internet PC's or other things they require a person, they require a user that will ask to do something. But e.g. we can take a look at one machine or set of machines that can measure something acquire some data automatically may be react on something etc. and do so some program, things by itself and report it somewhere, then we have started to speak about IoT.
Researcher: So what you are saying is like IoT is something that is autonomous, which can do computing, which doesn't needs human interaction, it could have but it doesn't necessarily need it.
SM1: Yes. It's better if there won't be any human interaction.
Researcher: There are like some sensors and it can report to somewhere.
SM1: Sensor is only one way of the sector where IoT can be implemented. It could be anything.0 Sensors are only data measurements, there could be some reaction, there could be some unification e.g. a lot of things within smart environment that could cooperate. It's not necessarily sensors it could be together make your life easy. Now a days if you would have probably heard the new wave of IoT its IoT within business, factories, smart houses, within smart cities etc. everything with smart prefix, it has also started to be treated as IoT hence it is extremely broad.
Researcher: That actually brings us closer to the 3rd questions what are the properties associated with smart Things?
SM1: It should be able to gather data, compute data, or react on some data like triggers etc. it should be computed or analyzed, processed without a user, so it should be autonomous and since we are speaking about Internet of things so The Internet, there should be possibility to report it to somewhere. May be...
Researcher: to communicate
SM1: Communication Yes :)
Researcher: Do you think these smart things should be identifiable or addressable in IoT context.

SM1: This is also very bright question because and yes and No simultaneously. They could be simply different ways of usage of these things. Somethings definitely should be anonymous. e.g. anything that you can wear, anything that you can allow to any 3rd party to identify and bound you as a person to this device and get some additional information about that definitely will violate your privacy etc. like GPS sensors, some heart rate sensors, but other can really help if I can provide this information like this piece of information from some gadget being taken from me, like e.g. smart houses if it will open door for me it will identify that it's me.
Researcher: So there is some trust aspect that you are point to.
SM1: Yes it should be
Researcher: So but you agree that it should be addressable otherwise it's not possible to communicate like the IP node
SM1: I think it should be part of requirements. It should be possible to switch it on and full possibility to switch it off. It should be really.
Researcher: So smart thing could decide if they are in or out.
SM1: It should be part of presets or configurations somehow.
Researcher: So far you addressing the smart thing is different from identifying it and identifying is more about privacy and trust. **SM1**: Yes. Definitely.
Researcher: Now it becomes more interesting since we come closer to to the theme Are you aware of any general constraints in Internet of Things?
SM1: General constraints as technology or general constraints as movement.
Researcher: As technology and features
SM1: Well..... Right now biz shows us that it's mostly embedded systems. Small sensors some SOC and its smaller it should be possible to fit and feasible everywhere in small and should not gather energy and space. It actually brings us to such reality that it is really embedded device with small amount of resources where we can have several threads and one modem and it actually ends up with very limited unit that process only one task and of course the task to measure or send something but not to secure it or not try to create additional check or boundary because it is very expensive from the resource point of view
Researcher: When you say resource what is that?
SM1: Resource is CPU power, battery, space if its small amendment for bulbs, if its door lock it has limited capacity for space that it can take. If it's NFC the it actually has limited proximity sensor that will be able to work. You have to literally touch it.
Researcher: So it means it has environmental constraints and then technological constraints and...
SM1: Yes, actually a tons of them ... laughter... Additionally there is probably another constraint, since there is hype around IoT... be honest. Ericsson reported in this year there are 16 billion devices which are not PC's but IoT something. So and this IoT something, small things, sensors, they usually are very limited

with resources. They do not how to work correctly with speeches, with routers. They can only communicate with real IP addresses. Its pity that only expensive ones have possibility to work with ipV6 where you can address directly.
Researcher: What is the reason behind this particular constraint?
SM1: IP4 is very cheap not cheap but easier since this technology is already in place. You can buy now a days if we are speaking about SOC there are 3 major players and all startups how they are doing money on this hype. They try to buy something from Marvel, Qualcomm or OTI already reference. They try not to do anything on top of it. May be a nice box, may be something to put it in commercial and that's all. Reference code that is always old because it was created several years ago to simply show that it works. And these startups they do not do anything. They immediately stopped to create any updates, they SW is old and no one think about because ip6 Well we cannot say that is modern thing... But you know that in Europe that several years ago we depleted all ipv4 stack. We try to buy them from Africa. All ipv4 addresses are from Africa. Actually I got this information from Sigma. They have some... probably I should not pronounce.... Laughter... They are creating several projects that require ipv4 for their communication. It is really problematic thing when we are speaking about IoT. It's still a very powerful idea that all the small things really have to have a connection to internet... Why
Researcher: So if there is no internet there is no internet of things?
SM1: Yes, kind of 11:51 and no one thinks that there could be another topology and they even should not be connected there, they can simply communicate with each other if they will be several.
Researcher: So it can give birth to new innovation... a new internet.
SM1: I am not sure if you have this question or not but it should be touched here. Finally I think in the start of this year Alliance was created one year ago but finally this year they started to discuss something that guys now a days every vendor within IoT, every company, every startup, etc. reinvent the wheel because they all need communication apparently, they all need some way of sending this data to collected because usually we are speaking about big data somewhere store house etc., they all have to find a way and all these company they have found their own ways how to implement communication, e.g. how will the small sensor send data, which protocol will it use etc.
Researcher: So there is lot of fragmentation?
SM1: There is no standard at all
Researcher: Do you think they use the standard protocols anyways? They don't use standards at all or they use multiple standards?
SM1: Starting with this new association, I think Qualcomm actually is in charge. They name it somehow with a strange name but the Qualcomm actually is in charge for this community. They have started to think about how to create some generic way to solve some standard tasks or goals. Communication, Security, Privacy, etc. Right now e.g. for BT, ZigBee, one protocol a lot of guys actually use this but majority do not use it and they use their own. speaking about the small sensor e.g. from Bosch it sends

directly open data, speaking about the e.g. Chinese small sensors they simply open raw TCP/IP sockets and you can get everything that you want. You simply have to know the port number, password is unchangeable... laughter... its generic it's hard coded. .. Laughter... there is no any other firmware and there is no possibility to change it and there is no open source code that you can modify by yourself so...
Researcher: I think you mentioned about source and that brings us to the next question. The next question is actually about the open systems so how do you see open systems and open source in terms of IOT
SM1: it's a disaster if you put it to use only one word a lot of how to say not really tiny but middle sized IOT devices they try to use Linux and do the Linux license they have to. They open the Linux kernel sources some of them even tried to open the device drivers but mostly binary blocks. But I don't think that someone tried to do a real survey but I think it's my kind of gut feeling that after first release may be second they do not update anything else. And for example even if you will try it later on update the Linux kernel you will get immediately The problem with the recompilation against this device drivers blobs etc. I have the same I have a Tegra 3 from NVidia. They stop support on 3.11 version. So nowadays it's extremely old one and device drivers they being blobs. Yeah I have Kernel and sources and I cannot move with anywhere else. Actually I cannot updated by myself. I can recompile but I mean I have possibility as a developer and I know how to do this but do these blobs it's completely useless operation for me. So they managed to bypass the law but as a customer I've been I think that I have been tricked and I have paid for this device
Researcher: So what you're saying is like even though they use open source but they don't have flexibility or extensibility to the code and how do you see customizability of the system. Is it important from open system point of view?
SM1: Customization. I do not know. To be honest because...
Researcher: you mention about the Qualcomm things Qualcomm SOC they buy different SOC and then they just take it as is and there's no possibility to like fine tune it further and not even change the password.
SM1: I do not think that really customization is really needed for end customers to be honest these pioneers who developers
Researcher: Yes we are talking more about developers here
SM1: Yeah for this may be but to be honest 16 billion IoT devices. I do not think that majority of them really are on developers shoulder. Of course it's regular people started to buy them and they won't do anything so I think they finally should be a way of or auto update or any possibility to change the firmware somehow but very easy if you are a member of 10 or 20 years ago that was pretty the same problem with the PCs when you've been able to postpone the update on your windows PC and then tons of viruses blah blah blah. Now I think that IoT has exactly the same situation. Exactly. If industry won't find a way How to force from the beginning maintainers to create a new firmware at least with security patches and updates and then users to update this firmware on their devices that will be always a problem. The

latest the biggest botnet was reported actually on the Internet. I do not know does it exist. But I think it exists still so let's say it uses. More IoT gadgets and devices than regular PCs. it's much too easy
Researcher: What is your view, Should IOT move towards using more open systems and open source code or its better if they remain proprietary and adapt to user needs
SM1: I really don't think that it matters .Actually it matters only the attitude from the manufacturer who ODM or any other company that will manufacture some of this and customers device. Will they continue to support it or not. Because as I said even if it's open system Yeah. Even if the Linux kernel is open and they even showed it somewhere and guys take it in majority of the cases it's useless.
Researcher: But it can help each other right? If the system is open for example like Linux I mean or Kernel anybody can patch and then you can build upon like someone.
SM1: Yaa but then they have to open everything. I mean not only Kernel but they have to open the device drivers and bootloader all possibilities to open it. Yeah yeah. If everything will be open then that definitely helps. For example like for routers or now a days. Finally this was changed and now on majority of routers you can actually unlock it and installed your own operating system and be really happy and change it.
Researcher: But that's like completely customizing the...
SM1: Yes exactly.
Researcher. But what we are talking here is more about like If we have open operating system and then things might go very quick like for example Android.
SM1: Yeah but business definitely won't be going that way. I don't believe that big companies decided oh let's open everything .They use and we already agreed that majority of the small companies startups especially if they have to provide a result immediately. ASAP yesterday .And that's why they take reference add some small features maybe as amendment to reference on top and they do not care about the film itself . They don't have anything to open.
Researcher: But do you think Linux would be a better choice for them instead of going for a proprietary system.
SM1. It depends from the gadget size if it is mid or big one then Linux is a very nice choice
Researcher: or Linux like Linux like
SM1: yeah but for small things of course it's usually something real time so free RTOS etc. and they usually they have BSD license that actually does not force maintainers to open anything so it's always a binary for you . And as I said from my point of view it doesn't matter will it be open or will it be closed it won't help in any way unless manufacturers will not have a will to continue to patch their devices to force users to update it or find a way. Right now I know that the reason even initiative to stop selling routers to regular people and there should be only ISP providers that provide you an IP address for Internet and they will provide you router as well. All the time together so it would be kind of a package and it seems that they are professionals .They will always update it and can install something there that will protect you from may be from the viruses and some filters etc. etc. . . .Is it good is it better I have no idea but I mean .

Some problems definitely can solve... laughter...there are lots of new problems once especially in some privacy.
Researcher: But let's move on to security & privacy .What are your views on Internet of things privacy?
SM1: There is no privacy. There is no security. Both of them. .. Laughter… of IP
Researcher: Can you elaborate .on that?
SM1: Security yeah probably you heard this
Researcher. Let's take it from security.
SM1: Security is well known joke. Yeah. So in abbreviation IOT S as stands for security and the reason it's not there so laughter... that why security doesn't exist. So it's easy .as we already touched this theme this topic... Usually it's not enough resources for the real security and especially and if we really need the open network connection we really have to think about security...
Researcher. So let's twist the question so what does security mean for you in terms of context of IOT.
SM1: If there should be some..... Well first of all..... we have to also touch the topic of What does it do this small gadget of IoT if it sends some sensitive information then of course this also should be some kind of hidden encrypted etc. .If it's could be open then we simply have to be really sure that the end to end connection that was established was really established between our gadget and the server that we really want to use.
Researcher: Trust management?
SM1: yeah kind of Trust management it should be in and if we are speaking about some pieces of privacy we also have to know that or to be sure at least that in the end this data won't go to any third party. And yes there a lot of practices how to achieve this using normal PCs using normal networks. But usually it requires resources for some piece of hardware or some additional CPU power or some 3rd party that will revivify that e.g. Kerberos etc. etc. some tokens, authentication additionally or some user input. But as we already know that we can enter some credentials or put the fingerprint etc. Yeah but since we already agreed that IOT at least in my sense it's something that can work without the user interaction so it should be somehow automatic. And since we already said that usually small tiny thing that doesn't require or doesn't have a lot of resources then it started to lack of CPU power and battery and everything to be honest for security. Security is the first topic that actually got that away from the IOT things and from the beginning I think how to say well we have to also remember how this IOT went in our lives. Usually this Fridge maintainers or TV sets maintainers or Stereo system maintainers. Yeah they had a lot of things but no one thought that they would be connected into the Internet. They do not have and did not have the expertise for their own security. They did not needed because it was standalone piece of its own maximum that it was able to do to connect the cables with some device of their actually company from their partner so it was trusted by default because there was wasn't any network. There wasn't any hostile environment that was peaceful nice open may be network. We cannot say network I don't know simply environment regular environment without any problems without any enemies. And now a days Yeah they have to add a

possibility to connect to the Internet that a word of bad things, viruses, hackers or simply full of people that simply do because they can do this.
Researcher: Where do you think that security is the most important on these smart things or the network or on the cloud or it's everywhere?
SM1: I think it's very close should be bound to the privacy. If the privacy is important for you or if these gadgets are really hold some privacy thing then security should be everywhere. If it's some information that you do not care it doesn't have any privacy price then probably we can start to speak about weak security or no security at all. I don't know but I believe if we are speaking about the GPS signal that could be send from me, I do not care to be honest as a person, any time and if it will be used later by some third party to analyze where I am going and where everyone is going and I don't know if they find out that oh take a look at this street after 8 still there are a lot of people let's make all shops open up until 9 I think it's a good.
Researcher: but they can use it for very weird things.
SM1: Exactly.
Researcher: Criminal activities as well.
SM1: Criminal activity but I'm more frightened about for example such cases when you are client for insurance company for 10 years. You do not have any accidents. You didn't have any problems before but then they found out your data that you start to be slightly lazier .That you started to be more attractive to somebody and they decided OK from that point this guy's probably will have a heart attack very soon. Let's drop him. You because they can. And why not. Actually they can predict something and from their perspective it's bad so it's a contradiction. It's a trade ....and since we cannot say that.... you have to decide all the time. Maybe if there is a possibility we have to use security all the time everywhere as much as possible.
Researcher: But how about heterogeneous system that is one of the traits of IoT. The systems are very different they have different security protocols and how will the intercommunication work. You can secure for example I can secure my IOT mouse as much as I can. Let's say if the TV is not secure then it's not end to end security
SM1: That's why I said it's very nice. I'm really hoping for some changes after this consortium is being created. That really decided to finally say it out loud. Guys we need some IOT standards for security as well.
Researcher: And why do you think people will actually follow them.
SM1: People who are quite good followers. It's really good defined especially if it will be good define low protected. And they will be nice supplementation from someone else for some 3rd parties and open libraries they immediately will be very popular.
Researcher: So what you're saying is like it's very important to have security requirements on IOT systems from start. Yeah so if we touch upon previous question so we discussed about the open systems

on IoT. So what you're saying is like it will be really good to think about security requirements from design phase. Even before setting up the startup and we shouldn't really think about how I can...
SM1: It should be mandatory.
Researcher: Yeah
SM1: really but it should be binary.
Researcher: That is good because this whole thesis is about how to create security requirements for IOT systems. I think you touched upon most of the existing security traits like trust management, authorization and authentication, key management in a way like How do smart things talk to each other and then we touched upon privacy, access control in a way. How about the revocation of device? What do you think?
SM1: I think it's impossible. It's of course very nice but it's impossible. I can see it in certificate world because it's all this revocation mechanism is also being created for good of course. Certificate KPI architecture and I can't see how that does work... laughter... For example if you take a look into Android it does not exist at all.
Researcher: But you said there is a need for switching on and off certain devices and that is almost like revocation? If something is behaving nasty then it should be possible to revoke it.
SM1: It could be also implemented in a different way. For example if you have to revoke something it could be changed within the whole firmware and you can update the whole firmware because usually it's one application that has everything boot application user data and communication module. It's one application with no internal loop. So it could be like that that something happened some security vulnerabilities some certificate was stolen or some server was compromised and you have to change the logic that there should be a new firmware for your gadget or for your this device that could be uploaded and it should be not on a daily basis and not really on demand but it should be some stable schedule that for example should be really. It's a part of a deal when you will buy something that was the next three years for this device every week we will tell you this should be updated or not like this. So you know that your devices are safe secured. Otherwise I don't believe that it could be like this. Like for example nowadays Google said six years long term support for kernel. This one sounds really promising for me. I hope that just soon will happen the same for IoT because nowadays it's so Wild Wild West
Researcher: So what you're saying is like we should think about security from the beginning from the start but if there is no updates like maintenance then there is no security. Right?
SM1: Yes. It's the situation nowadays. If you would take a look at the software, Linux, open software this is the only one we can analyze on the latest routers latest 30 routers that being actually on the latest defcon and half of them being hacked actually on the stage immediately and live. The software download was there-four years old. We have it open we have a whole bunch of security patches for everything. Yes. No one cares. And they're have been actually not something like I don't know Chinese no-name but there's been a lot of brand names.
Researcher: I see. And how do you see where should the security be implemented on like software level

or should it be more integrated in the hardware layer.
SM1: There is one thing where I can see it and there is another thing where it could be applied. Of course it should be Software security without hardware support usually is a weak security. It exists. It helps against script kiddies but it definitely won't stop professionals.
Researcher: Is it possible to have hardware security in IoT?
SM1: It's another thing we can see that if you remember the first IoT tries yes there was always hard drive for example the washing machine. I remember I had one and it was big. There was a full RJ45 connectors so it was really small computer. And now we can see that it is shrinking smaller and smaller and smaller. And then it can actually do a lot. So yes, I think that soon there will be a lot of things like integrated SIM card not something that you can switch on/switch off but really integrated SIM card that really could be used as a secure element there could be crypto quite fast, Small chip, then finally really cheap . And if you will buy it only for this operation yeah it will not be secure to store information for n long term. Yeah with modern powers with the cloud solutions you can decrypt it after several days. After several days this information will be old. So that's why no one will go for this. So you can postpone the problem maybe....I really see that it will go in that way that people will stop to believe in these small startups without any possibility to support their products they will understand that the startups actually started to provide something only to get a nice deal from Google or Facebook or any other guys who will be able to buy them. I start to believe in big companies that really can say yeah we will sell you this this and we will also sell you the support new firmware, security updates and no one will care that it's open or closed or any other solution like this.
Researcher. I think we've touched upon like two other questions which we had but we can go in details.
SM1: Laughter.... everywhere
Researcher: But feel free to go in like technical details.
SM1: Absolutely.
Researcher. I think the other question was like why you think considering security & privacy while designing IOT solutions is critical. I think we have partially touched upon it. And actually the other interesting one is, what are the challenges you see in the existing security mechanisms? I would like you to go in-depth of this.
SM1. Think we have enough challenges.
Researcher: So basically what I'm saying is like let's rephrase like all these questions of if let's say if you were the architect for this new IoT startup is just going to launch some nice sensor which gathers data, processes and then sends it to the cloud. And so for this kind of system what would be your thinking process like how do you want to see security in place. Let's design some system.
SM1. It definitely will be a trade and always will be try to find a balance between the enterprises because of cost. From the beginning you would like to put in everything but immediately your price will go up to the sky and then you have to start to remove a lot of things. something that bring to the software,

something bring to the some updates maybe in SW once again but remove as much as possible from the hardware because it's the hardware piece is mostly the costly one. I remember in my company that used to work before we had a discussion about which kind of chip we have to use for the GPRS it was about security actually and that was point to point channel implemented in one chip and the same chip from the same company and that was only 50 cents US dollars 50 cents actually cheaper without this channel. And I remember that sent to my boss of course was have to take this with channel implemented because it will be for me as a developer because I was responsible for the communications would be much easier. Channel was already ready in the hardware. He said we have 70 million devices so every device will have this chip. He said imagine how many salaries a month I can pay you to implement the channel. How many months will you need? Well we're going to need - one and half to 2 maximum. Yeah and then I will implement it because I had some piece of code. So just go and implement this. That's the thing that's the real situation actually in the market. It was a payment terminal for those security cars. So the same the same approach will be exactly in IoT. I cannot see any difference right now nowadays. The only one probably exception is that it's extremely limited resources and maybe some good things that you really want to have there. You will not be able to put there for example RSA operations they're very expensive from the CPU point of view and the TLS probably will be if you would like to open it will be quite difficult. And especially the modern TLS with the keys at least 2048 bits.
Researcher: So what you're saying is like the existing mechanisms that we use on PCs and mobile we cannot use as is in the current state.
SM1: We can but we have to think about the different architecture. Finally this idea actually started to be really how to say.....when the program started to be a really normal is a bad word obvious I have to say yes for IoT developers that not every sensor or not every gadget not every piece of this network should really have a direct connection to the internet . Yeah. Yeah. So finally this eco-system will start to have like a gate. Usually it's a normal PC that have a possibility to go to the Internet that could be protected. It's only one end point. It really shrinks the security surface to only one connection that you can really protect that you can really maintain that you can really update but internally it has a connection. Sometimes even open to all these bulbs, locks etc. etc. etc. And from that point of view all the small gadgets they can draw any fear of lack of security or other stuff. So finally we can see this trend in the IoT world for example IKEA latest product. They have a small gateway that will be connected to the Internet that will have RJ 45 connector. And it has a Bluetooth adapter that could be manually configured to be connected to this box on the bulb. You have to put manually some special number. And then manually you have to input this number into the BT adaptor and then they will
Researcher. So it is like network of network so we create a gateway and not expose the vulnerable devices.
SM1: So real Internet will not be able to go inside the IoT internal cloud.
Researcher. So that is like a quick fix for...

SM1: I do not think that it's a quick fix I really think it's a solution.
Researcher: Yes but that's more for the network of devices but there could be some IoT device which is on street.
SM1: Not at all a problem. These sensors also have to connect have to gather the data send to some central hub centralization unit that could be act as a Bastion that could be treated as a fortress.
Researcher: But let's say all the lamppost on the streets were IoT lamps then this solution is not practical because there will have like a sim card which will actually communicate with or there could be Wi-Fi.
SM1: Yeah. From that point of view probably not of course.
Researcher: Or connected cars for example .There's no other option but then you have more possibility because car can have
SM1: no no no no no. Car is very good example because car has so many different sensors and for example probably your brakes definitely should not send any signal to the Internet. No one should know in the Internet how many times did you open and close the door but all the sensors that they can collect this data and store it inside the car and the results of one small actually block that will decide what will I send what will I leave here what will I put in the local data base and what will I wait for my actually hostel. I don't know.
Researcher: So in your world connected car is a reality it's not ten years ahead in future
SM1: I had actually conversation with the Volvo guys and they are really discussing right now not discussing they already have started implementation of this module that will speak with different sensors or actually sensors will speak with this module. He's only a listener. He listens all these data and then he has policy kit what should go outside what should not go outside in any other way even if it will be asked kind of like that. He knows he's the modem manager. So only he has a connection to the Internet. No one else in this car actually and it's a very nice decomposition. Sensors knows how to get sensor data and they shouldn't care about anything else. This block is a security master he knows how to deal with security he knows how to update itself. He knows how to establish the connection itself and everyone has to do their own job. That's the thing that's the problem with IoT nowadays we're trying to fit in the small sensor everything. And that's why if you are spreading your attention and your power everywhere probably you will suck everywhere.
Researcher: So what you're suggesting is like we can have a tiny OS running on like small IoT devices like smart things. But then we should have like bigger
SM1: concentrate or something like that.
Researcher: Which can run rich OS. And then there is like cloud which can actually do heavy processing, e.g. machine learning. This is actually a good architectural model.
SM1. It already exists and as I said it's very ... I'm really glad that it finally became more understandable in IoT world.
Researcher: Because I didn't came across this kind of architecture in my literature study.

SM1: Just recently there was a hackathon. Have you been there in Malmö for smart city? It was discussed a lot over there. Actually I've created by myself a small watering system at home. So there is a raspberry pi that checks the soil density that checks the temperature that checks the humidity, that checks the water level and it actually hose the pump and it decides by itself. From the beginning I configure it actually so it should when the soil will say that it's dry it has to pour such amount of date such amount of water if it will be already empty tank Then it also should shout and the only thing that it can do is send an android message to me . So it even doesn't have a feedback. I really closed it down completely. So this small tiny Raspberry Pi It's like a monster works with all the sensors graze information knows how to do it and completely autonomous. And only in the end can tell me what it did. Why did it take this decision and if it should be something ...how to say.... announced like empty tank or completely dry soil and blah blah blah... some malfunction then it will shout slightly louder. That's all. That's I think it's a definition. How and where should it go?
Researcher: I see so I have this last question but maybe I have may be some more questions. Are you aware of any existing security techniques within your organization that can address challenges in the IoT?
SM1: I have no idea to be honest
Researcher: but I think with your previous answer with this architecture and hackathon, I think that is like kind of addressing my question in a way.
SM1: It's mostly not really techniques but is mostly about mindset. The leaders in IoT are right now they are trying to push the mind set to this already that I have mentioned several times. Please consider is it really necessary that every sensor or every gadget should have a real connection to the open wide network really is it needed? So you have to start to think like Linux way that close everything first and then open only what it's needed to be open like that and not the opposite. Because from the beginning we're seeing that every fridge every oven wanted to go directly to the Internet required a direct connection. Had problems with the routers etc. . . . Now finally we can see its opposite situation. And I think this technique this mindset should be right now on top before any designing before. It really removes a lot of questions about security immediately about maintainability etc.
Researcher: So if you want to put any requirements on these open IoT systems security or privacy requirements. What would that be like? What is the key thing that you want to have?
SM1: I think it's a general goal of what do you want to achieve. You have to really say I want to create some IoT stuff because I am interested in IoT because it will help me in that that and that. Using these goals you can also start to decide for this I have to send that or for that I have to achieve that and these goals will put constraints immediately on your design or force you to open something or to have something additionally. Think it should be like that. You cannot put some general practices here. DO not do this or do not do that, etc. sometimes it's not applicable. It's really per device or per idea
Researcher: Ok so it's not like I want to have trust management in IoT systems or it should always be encrypted data transfer.

SM1. I do not believe this you can achieve the same goals in completely different ways but that's the problem now a days. Every company tries to achieve their goals in their own ways.
Researcher: But general guideline could be like think about if you have privacy then think about the trust, crypto, etc.
SM1: Yes, I hope it will be like that but it will be more really generic highlights. If you are sending some private data of the user then you have to start to think about GDPR. You have to think about possibilities to erase this data. It will give you an insight if you go on this unknown field it will immediately bring you and this amount of questions that you have to challenge that you have to solve, answer. May be it will stop you to open or amend so many functions to your product from beginning.
Researcher. In general open systems they usually consider they consider flexibility, customizability and extensibility... Do you think when we talk about IoT security should be like...
SM1: I think it is a must characteristic
Researcher: It is completely missing in current models. That is my thesis it is about adding the missing characteristics to open secure IoT systems. Is there any last statement that you want to make to the IoT community and developers?
SM1: Probably we discussed everything, covered everything and slightly story and slightly generic questions and technical stuff may be that was not necessary. I think that the end word here is that actually on the end customer side that the only think that I would like to recommend them if there is such possibility or availability of some platform where I can recommend something. Do not buy something that was not tested by some 3rd party company with professionals not only security but simply technicians. e.g. there was a huge scandal about sex toys you can also say it is part of IoT because it has Wi-Fi and camera etc. and there was a huge problem with the WIFI because the name of the access point was not changeable so you did not had possibility to change it and password as well. And if you remember there was another scandal with Google when it actually did Google street view they also scanned WIFI network and someone created an additional map that you can apply to Google maps that shows everywhere WIFI network with this special name and there had been a lot. So you can identify houses where this sex toy was used. It was embarrassing. Slightly later, Toms h/w tested this device, they opened it up and they tweaked the firmware and they found so many bugs, there clear statement was guys do not use it it's a so buggy. It was extremely popular and lot of people started to buy before any official security penetration testing was performed.
Researcher. Does the user even know about all this? My mother or wife will definitely not know about the refrigerator. What can she do? She cares about security but will not take extra step to check security state of the device. We really have to create a system where users are not well-versed with security There exists digital divide in IoT.
SM1: It's like I wanted a device and then comes surprise with nasty things.
Researcher: Thank you so much **SM1** we are right on time. It was such a pleasure to meet you.

Appendix B: Interview of SM2

Researcher: The first question is about general understanding about you and your role and how do you contribute to IoT?
SM2: I work as an architect for R&I department specifically the research and standardization part. Which means that I am not bound to specific project but available for project as specialist and I am also looking at emerging technologies and applications within security and IoT.
Researcher: so it is like a very broad view like system architect
SM2: Yes with some research part as well
Researcher: Are you working on full stack from h/w till app.
SM2: sometimes I am not really web guy or browser security is not my strongest thing but I am looking into that as well.
Researcher: when you look at IoT you look at all the layers.
SM2: No, if we look at holistic security then we have to address everything. But for cloud part and anything from TLS and upwards you have more standardized tools available. Then its matter of how applicable they are in IoT domain and what does the future holds.
Researcher: What is your view on IoT? What does it mean for you?
SM2: IoT doesn't mean anything to me it could be anything.
Researcher: So it is like internet of anything
SM2: yes. There is no real definition of IoT. Is it an android device? Is it a sensor or is it an actuator?
Researcher: How do you see when people talk about IoT?
SM2: Within our department we have almost all of the interpretations of IoT. We have range of applications and project and some of them are even below the internet part since they do not have direct connectivity so they need another device or gateway in order to reach internet. If we are looking at BT tags etc. We have other projects like Nimway which is more like cloud solution which they don't have any embedded components as core part of their system.
Researcher: You said some of your projects have devices that are not directly connected to the internet. Is it some kind of design pattern or is it consequence of user requirements?
SM2: It is consequence of capability available for the device in question. If you are going to be connected to internet you can do with wire which is connected with power but usually we are talking about battery powered devices. If we have LTE connection it will have implications on power stamina and also cost and so on and so on. The ideal view is that SONY is heavily involved in connectivity and research and standardization are part of 3gpp and other connectivity standard body and they are very keen on adopting the view that we should have BT but should have 5G which will enable even the lowest kind of device to connect to internet and run on batteries for sustained periods. So that is the future vision from connectivity

point of view of internet. If you look at cloud provider's point of view like Amazon and Google they are not really targeting that kind of power profile. Well they have internet is anything about TCP basically in their point of view. But if we look at 5G use cases it may be that you cannot even use TCP due to the connection characteristics.
Researcher: What are key properties that IoT devices or systems have?
SM2: Since the devices are going to be connected there is going to be security issues with your device and data for your device. That is one thing. But I also think that history recently has demonstrated that IoT devices can be threat to internet itself and services for other people because it is shared resource and there are some sort of assumptions on how the devices should utilize the shared resources of internet that can be violated and can bring down functionality which is threat on critical infrastructure for society. If large part of internet is brought down by DOS kind of attacks or whatever as demonstrated by these Chinese routers it's becoming issue not just for owner of that router because he did not experience much more than lag in this device but DNS that was targeted made it impossible to reach things like Amazon, Netflix in parts of US which is very serious. What happens if your power company is dependent on internet infrastructure and someone can attack it? It's like back in days when radio emerged you have type approval and certification, you cannot use the frequency spectrum unless you are trained to use it and your radio is guaranteeing to stay within its frequency range. Now with the internet you can connect anything without any certification to your ISP and how do you deal with it.
Researcher: Is communication the key in IoT. Does it need to be always connected?
SM2: Well, you have other aspects for data at rest if you are looking from your device point of view. If you have your thing mounted in the ceiling in public building that presents also some degree of challenge for you to secure your device and your data.
Researcher: What is smart thing to you and what properties does smart things have?
SM2: Well, I don't think that IoT are necessarily smart things because the smartness if probably associated with heavy computations and that's why u probably have a system that have sensors as nervous system and cloud is a brain but for the body to work the communication between your sensors and actuators and your brain must be up and running otherwise you will may be trick your brain into doing something which should not have been done.
Researcher: So do you mean that smartness is not in the device itself it could be distributed
SM2: It could be ... yaa... and then whether you want to have it distributed like a peer to peer technology or you want to have it in cloud environment that's also part of the system because cloud is single point of failure but if you distribute is more resilient to targeted attacks of course and you also may be issues like latency where you want to have edge functionality which is close to your devices rather than in some data center.
Researcher: Yes, talking to cloud is sometimes is really slow.
SM2: yes

Researcher: So the smart thing in your opinion is an interconnected mesh and do they talk to each other or it's usually like...
SM2: it depends on the level of peer to peer you have in your system. But I think the traditional IoT sensor grids are more like they talk to cloud.
Researcher: Do you think humans can be replaced by Smart things
SM2: That's more of an AI question rather than IoT.
Researcher: Usually these systems are autonomous and it's closely related to privacy and security issues.
SM2: Yes, there is definitely machine to machine communication emerging and that opens up new dimensions of complexity of course. If your HW is communicating with other h/w without your interaction. It's one thing to have a dedicated point to point where you are reporting your data but if it can take action autonomously is a different story.
Researcher: Is autonomy a key property of IoT?
SM2: It depends on your use case and your profile and system. Self-driving cars definitely needs to have interaction on car2car level in order to make that system work efficiently.
Researcher: How about the addressing of these things?
SM2: The addressing is and the privacy part of the thing. I think it is one thing for the sensor that is not associated with humans in terms of privacy. If Sony puts up thermometer in every room here it's not really something that is associated with person. But if something sits in your car its different story from privacy perspective.
Researcher: Will there be need to locate these thermometers?
SM2: Yes, but if they are attached to Sony building instead of attached to humans, I don't think there is privacy issue. We have a project about tracking of goods and there is a discussion about privacy of driver carrying the goods because he will be tracked because the goods are tracked.
Researcher: Is it like chain of privacy issue.
SM2: Yes and some other projects we have is about personal thing reporting data but it's still bound to you like smart band type of device.
Researcher: What are constraints in IoT (Technical, technological and not business)?
SM2: Battery stamina is key thing because it puts boundaries on how much computation one can do and also puts boundaries on how much data you cans end and receive. If we look into type of devices that we deal with e.g. LTE kind of devices the cost of modem and complexity of modem and security requirements for the cellular network are already relatively high and adding h/w capable of doing sensible security scheme is not that serious. I mean it's not like you will have to cut the cost to 1 cent because the cost of your connectivity be already be so high so I don't think that will be the problem.
Researcher: So you think security modules could be added with little extra cost and we have future proof solution?
SM2: Definitely. If we look at the ARM microcontrollers, the ones we are seeing in relation with modem

and connectivity are like a Cortex M4 and upwards because the later ones will have more capability. On Cortex M4 you can run PKI in SW. If you are targeting lower cost even Cortex M0 you will probably be not running public key, elliptic curve efficiently on such a device.
Researcher: Do we actually need these security solutions on each of these IoT things? Can we have some different kind of architecture?
SM2: Yes, that's when you look at things that don't have individual connections that use a gateway. If you have something that is communicating with BT to something that is connected to the wireless internet it's a different story and it brings interoperability parts. Because if you want to allow someone to connect a But device to your hub you must accept or restrict a devices according to your need. There are standard BT association model are known to be weak. The key exchange that takes place when BT devices are getting paired with or without passphrase is weak. So if someone is eavesdropping during that phase they can extract your long term BT keys and they can eves drop on your BT link.
Researcher: Is there any alternative technology that can be used?
SM2: Yes, there is already stronger versions of BT association where you have an out of band provisioning of keys where you can inject the keys into the devices or you can exchange over NFC which is supported by Android and some of the NORDIC BT platform then you can have stronger pairing of devices because you are not sending BT keys over the BT link. You are sending it with NFC or QR code but then you are restricted with what you can connect because not much of the BT h/w supports that association model.
Researcher: So there are ways to overcome power and memory constraints but at the cost of security.
SM2: yes, even the BT h/w from Nordics semiconductors which are popular among our prototypes are capable. It has a microcontroller which is usually Cortex M4 and they have in some cases the crypto IP from ARM which means it can run public key cryptography accelerated in h/w.
Researcher: What kind of IoT systems the kinds of devices you are talking about where we can find those. Do we need them on b2b2c kind of devices? Do we need such security on these devices?
SM2: No, that's a different story what you need but I mean if you look at it from threat modelling point of view it is usually not obvious what happens if your temperature reading is spoofed. If you have a complex systems it is not always obvious to say that this we don't care about so I think that unless you are designing a specific platform for a specific use case where you can say that there are no such constraints you should anticipate the need for securing your communication. If you look at HTTP google is driving hard for every website to turn into https and the biggest impact for the website is that they must get the certificate from the domain. I don't know the cost for that really but it's something that Google is promoting because it will prevent things going on the internet when you are communicating with the web server.
Researcher: So how do you see the openness in IoT or open systems or open source?
SM2: I welcome open source because it will allow sharing and interoperability rather than having patents

and proprietary schemes.
Researcher: Is it different than standardization?
SM2: It's more like de-facto standardization. If something is freely available and of good quality people will use it and then it will.
Researcher: People tend to fork out open source
SM2: That's another thing but I mean if it's reasonably maintained or has confined use case then people should not fork out
Researcher: If we get lighter Linux version, is it something what people will go for?
SM2: Well. Yes possibly. Linux is a good example of where people fork out... laughter. It's heavily used but if it's the right thing for IoT device is not obvious because if you have really resource constrained device you can run Linux. You cannot run it on Nordic BT controller for instance.
Researcher: When it comes to openness you said you welcome that. When should we decide if we should go for open or proprietary solution? Is it at design/architecture level or it's already before when we discuss IoT concepts? How do we make choice and what are the reasons for choosing?
SM2: When you put it like that it sounds like openness is sort of an Eigenvalue i.e. you should have it but you don't really know why because it could be good to have it in the future. It good be thought of as a mark of a good architecture to be open.
Researcher: Right now in IoT everyone is having their own baked solution.
SM2: Well, I think that when it comes down to openness there is a boundary when you come into security part of openness. You cannot be 100% open to everyone and still be secure. I mean there must be some sort of trust anchor or authority or whatever if you have system with limited access. Question is who would limit that access and how. Assume your thermometer is available to everybody then it's open so you don't need to care but if you want to have it only to selected members how will the enforcing of that mechanism and election take place.
Researcher: Are you suggesting we should start with completely open system and then think how we should control the openness.
SM2: Yes, because if we look at it from M2M communication or P2P system then you are having some aspects of openness or may be democratic systems. But if you look at it from more traditional systems cloud point of you typically you don't have that much of an openness. If you build the service on AWS they will give you the tools to lock down the service. And on the other hand you can give tools to open up access to your service. But it's still something that is under the control of AWS rather than it's not open as in the sense of bit coin which is extreme in terms of openness. Which is also trying to sort of led your target being democratic but with some security properties. Which people have also been adding the buzz words of IoT and crypto currency in terms of boosting the combination of the tools saying that that's the future of IoT which I can firmly say it's definitely not. It's not even feasible.
Researcher: Do you believe blockchain will be solution for trust and authentication in IoT?

SM2: I definitely think that the current ideas of blockchain are facing a contradiction in a system that should be efficient open and secure. I don't think you can have all the three of them at once. And it's pretty obvious if you look at bitcoin its open and it's totally decentralized but it's not efficient but it's probably secure. But it is not efficient. So if you are going to edit bitcoin blockchain you need render farm in china to have processing power. You need vast amount storage and bandwidth. That is definitely not IoT so I mean there is it's not possible to run.
Researcher: But if we scale down the number of connected devices in the chain then we don't need big blockchain.
SM2: If you have 1000 nodes of processing power which is supposed to protect your data but if an attacker has 10000 nodes you will be vulnerable which is what bitcoin is still considered as golden standard because there is lot of computation power going into it which makes it hard for someone to come from outside and over take that power. Now there are other approaches on how to build a system like bitcoin and few of them actually which are built from bottom which are supposed to be applicable for IoT. But whether they are secure remains to be seen. Even by now bitcoin is not fully understood in terms of all of the aspects since it is not based upon a mathematical theorem which can be proved or disproved. It's more like a system with a large number of dependencies but there are lot of work in understanding these kinds of systems and modeling and be able to compare with each other. Eventually we will see if there is something that is applicable but at this point I would say no.
Researcher: What are your views on security of internet of things and key security issues in IoT?
SM2: Bandwidth, CPU power and battery are all constraints on cryptographic algorithms, key sharing etc. The number of devices makes local maintenance unlikely.
Researcher: Why do you think considering security & privacy while designing IoT solutions is critical?
If you were given to design a secure and open IoT system, what factor would you consider during design? Any key security & privacy characteristics or properties that you would consider, e.g. Trust management, Key handling, authorization, authentication etc. etc.
SM2: Current generation of devices/systems typically consists of a fleet of devices - owned by some entity, reporting to some central system. Here the binding is one key issue - agnostic production of devices that can allow a user to on-board them into his context. Here there is underlying assumptions on trust relations that can be used to resolve say key/certificate validations. For systems with "machine to machine communications" - there will be several trust issues. Certificate Authorities and DNS are by some seen as too centralized constructions with too much authority. So distributed ledger technologies may be applicable to such systems.
Researcher: What are the challenges or constraints in using existing security measures on Internet of Things?
SM2: For a device with 5G type of connection the modem will mean a baseline of cost and also

performance. So there is not so much cost that can be saved by using primitive HW. Also the modem will provide basic security for the radio network. But the planned bandwidths for 5G narrow band cell edge is extremely low. Established techniques such as TLS handshake/key sharing is an extreme overhead.
Researcher: Are you aware of any existing security mechanisms within your organization that can address challenges in Internet of Things? How confident are you in these existing mechanisms? If not, what measures can you suggest?
SM2: Yes. We follow standards in both radio network security and information security. The biggest problem is fragmentation: "Internet companies" such as Google/Amazon are quite separated from Telecom companies such as Ericsson/Verizon. This means that the solutions used by Google/Amazon vs Ericsson/Verizon are sometimes orthogonal: Protocols built on top of TCP/IP at Google level is quite different from challenges addressed by Ericsson/Verizon. Hopefully address space of IPV6 and new power save modes in the radio network will mitigate these effects.
Researcher: Any final statement you would like to make to the IoT community and readers of this thesis?
SM2: I think we can expect more regulatory requirements. After the Mirai botnet the department of homeland security sent out a query to survey how companies are countering malware threatening the internet.

Appendix C: Interview of TS1

Researcher: Let's start with the introduction of your company and what is your role and how do you as a person contribute to IoT? We can go technical in depth, it's more than welcome if you even talk about lines of code.
TS1: This is TS1 from Tec source and we are into green IoT solutions we are bringing value for industrial IoT and energy and e-health sectors. We working with both products and solutions for our valuable plants in South Sweden to start with. We are actually offering our solutions in Swedish and Danish market in the coming years. Overall my role is that I am XXX of the company and I have the responsibility to take care of technical operational elements as well and as a part of this interview like where Researcher wants to make analysis on how security is valuable in IoT and being more technical person than business person, I see that security is the key for IoT to succeeded and we do see it is as a very valuable portion of our offering without that we do not see IoT will fly or IoT will be able to take off. The reason is also that, we do go for business critical applications, so when you talk about business critical applications then you've to be more careful. If I talk about the process industry, a small breach in data security or even a small breach in something could also be misleading.
Researcher: Does it mean you are in industry 4.0
TS1: Industry 4.0 is the German term for it and we have something similar even if there is no catchy name for it in Sweden. But we are in line with industry 4.0. What the automation, how the automation is being brought into life with modern techniques like wireless and wide technologies. We also have few medical devices which are also part of our IP.
Researcher: So you make like hardware module and then you have software
TS1: When it comes to our offering being an innovative company, we are starting from sensor, hardware as well for the communications platform and then the firmware and the application as well. We are taking care of the whole value chain. The reason is that these are all getting integrated, tightly coupled and they are really coming close and closer. You can't really decouple them.
Researcher: Let's move on to the actual internet of thing. What does it mean for you?

TS1: Internet of things has been there for so long it's nothing new that you know we are in terms of when it comes to practice and not the terminology. Term is quite new in the market but its still connectivity. But now we want to monitor multiple parameter and not just mandate parameters. In that situation where they are multiple wireless technologies that can be saleable but a very lower business cost as well. That would mean that we're going to have millions and billions of devices being connected. In terms of business use or more of business use. There might be some consumer level but on the other hand but those will be very less in volume compared to business applications. Let's take the Malmö city and if they want to have like a million sensors to monitor the city in the coming years that's a big business case because they want to optimize and automate everything.
Researcher: Is this only for B2B or B2B2C
TS1: When it comes to primary business it is B2B but in the end it is B2B2C actually that happens because it's the consumer who is actually getting benefited. Even if you use for an industry who has at the consumer. If you make a car who is going to drive it, humans? So it is human centric applications that are being built.
Researcher: But industry 4.0 is more about the atomization of industry processes and then they consumer part is missing.
TS1: The consumer part is missing in a way but I don't say it's missing because it is delivering towards consumer because you are automating a process, so either you are saving energy or you are optimizing the cost and the product that you make is going to consumer.
Researcher: So there will be an impact on the end consumer anyways.
TS1: There is more need of IoT, without a human element. So human is the one who is going to get benefited at the end. From Techsoft side we see that human centric applications are going fly. If I make a solution where the industrial maintenance manager need not really worry that you know, then in the end he's getting better productivity in an industry, as well as he is also not really worried too much, e.g. not need to run in the floor like anything.
Researcher: So from your perspective, human is like in the epicenter of IoT no the smart things
TS1: Smart things are tool which is used for human value driven applications.
Researcher: That brings us to the smart thing. What exactly is smart things for you and what are its properties in your perspective.
TS1: Now a days we bump into smart city, smart health care or even like smart grid solutions. If you take smart cities we're talking about carbon neutral society's coming in 5-10 years. How do we really achieve it? If you talk about the EU or US or Asian markets, there is a bigger scarcity of lot of natural resources itself now a days. When resources are scarce you need to be more organized and more optimized. That can be only possible when you have more data around those. The way to get this data is using smart solutions in

these smart cities.
Researcher: Is it more about monitoring and fine tuning the user behavior?
TS1: Monitoring and controlling. Basically monitoring is of no use because some big companies do monitoring but if you can actually control using the monitor data so that's where the main value comes.
Researcher: Do you mean controlling the smart things or controlling the people themselves?
TS1: Controlling not the people but the process. Cape Town is out of water now and if you know like how to optimize or where you can cut down your water usage instead of just realizing at the last minute. Delhi has heavy air pollution, these kind of problems can be solved using the smart things actually.
Researcher: If we go back to the original question from the properties point of view what you're actually saying is that there should be some way to communicate.
TS1: Communication is basic. Without communication there is no IoT to be more precise
Researcher: Then you mentioned Computation. So we do some calculations and then you control the process and then there is like interaction.
TS1: Data analytics is the key. Without it you can't really know. Grabbing data is simple but the main value addition or the main important part is when you analyze this data. When you analyze in the form of smart algorithms or if you're have an energy grid and you would like to know like really you know what you say EU is after saving each Kwh of energy that you consume, if you can. And there are processes that can optimize. You are getting the data and you can apply in one of our application we actually know if you need to add or remove capacitance in the factory. We can increase the productivity of the whole factory and reduce the cost operating cost.
Researcher: Is there any autonomous property in IoT? Autonomous decision making. Does IoT system needs to be autonomous or it has to depend on user interaction?
TS1: From my perspective, it should be a bit semi. Of course it's always best to have automated most of the time taking self-decisions. But at some point of time human interaction might be needed. But things are also getting more towards more of an automated things or full automation. When we talk about self-driving cars, taking control of self-sailing cargo ships.
Researcher: So does it depends on the domain where IoT concept is applies? If you wear a smart band then full autonomous thing is needed but if it connected cars then semi-autonomous is better right?
TS1: If you are in north of Sweden you would like automated snow cleaning. You don't want to send people since it's much easier in -40 degrees.
Researcher: Do you see any technological constraints.
TS1: I don't see constraints but I see fragmentation when it comes to technical technology itself. But at the same time instead of having fragmentation ... When it comes to visualization of what is going to happen in the next five years, what I see is that there are constants definitely some of the protocols are not security

complaint or there's are possibilities for breach. But as we move on as the technology get popular the technology breach will be filled up because they will solve it. When there is more importance for particular thing, it's more prior then they obviously have to solve it somehow or the other.
Researcher: Can you be more specific on fragmentation?
TS1: Fragmentation in terms of what technology are we using e.g. BT or wireless or wired communications. Interoperability will also be some sort of problem. Of course on application one can do many things but there are bigger organizations the alliances that are driving forces behind these technologies. It's very simple the bigger muscles they have further they can push it.
Researcher: How can we overcome these fragmentation issues Do we need to really worry?
TS1: I don't think we need to really worry about fragmentation. The reason is that now during last month there was company signing a deal where they can know that the toilet paper is finished, i.e. a smart toilet. They are using some short range technologies for concentrators. When we're talking about with this millions and billions of devices, not every technology can fit for all these devices. Short range can fit here but when you to call from Malmö you can't have a cellular modem for every of the device which is very expensive and even the monthly subscription for the SIM might be expensive.
Researcher: SO do we solve the interoperability issue? As you say there will be some level of fragmentation in the market no matter how much we solve it then how do we actually solve the interoperability problem?
TS1: interoperability when it comes to protocol itself you can't really solve that. But if you are having data concentrators, e.g. MQTT or JSON structures all these things then it's a pure data where you apply smart algorithms. What we always talk about is be technology neutral. Why should we actually care where the data comes from as long as it is secure and reliable?
Researcher: Okay, so what you're saying is that all up to the data layer you can use whatever technology you want but when it comes to the data layer where we actually communicate between smart things then it should be in some standardized format. But even on that layer there is fragmentation?
TS1: That fragmentation comes from the vendor who is part of the toolchain or application provider. E.g. Microsoft, Amazon, IBM, these are the ones driving fragmentation part. I would say like looking from the consumer market we need not worry too much because the volumes are bit less compared to this because you might buy something fancy but you might be only fond of it for a week or two and then you are not fond of it anymore. But when it comes to this business process and business applications, they don't mind paying extra Tools like Azure, etc., they have very powerful tools but at the same time it's also expensive to use those power BI. So in a way that is a selection. Let's take Sony, they have multiple vendors like Qualcomm or former Ericsson, they can buy the chipset from anyone but in the end what they're making is like device that can be sold in the market on their brand. There is also a big motivation or big drive from

Europe where they are going for open frameworks. There's a lot of projects ongoing, e.g. 5 way and it is a European initiative and now they have opened new hub in Delhi, India. It's an open framework, open data and open things. Open data is good for smart cities but when we talk about industry then it is not open. One of our client wanted to have a closed one they don't want to have cloud for example. The reason is that they want to secure their own applications that they want to secure their proprietary things.
Researcher: My next question is about open systems. What exactly is the openness in your context?
TS1: As long as we can get the trends that is good you know. If I know that there's so many people going this way which has been working all the time so that's a good information for me to know so someone can follow that trend or that information. Rather than saying that this guy's is particularly doing this. More like hiding and being anonymous.
Researcher: What about giants like Amazon or apple for instance, if they come up with some IoT solution and many people will be following them so does it still fall into the category of open system because they're usually close ? They don't open-source their tools.
TS1: That's again is a business strategy. I don't say it's open thing actually because it's more like changing habits, for example, we are again coming back to B2C sort of mode. So changing habits is not that easy for someone e.g. someone is used to MAC, iPhone, etc., because they like it for certain reasons and certain elements or security of lower power things.
Researcher: We were more on the development front. So from development point of view, i.e. writing apps for apple, it's a very closed system you do not get access to code, what you get access to is API's but if you go for Android then you have access to AOSP and developers knows how their app will behave on Android based system because you know what the system is. That is completely open Linux.
TS1: It's more like clock brands. If you go for Armani or normal brands. Some people like the way Apple does certain things because they trust the brand the way make it secure. The Swedish market is more into Apple ecosystem, they like that way because they see that it is more secure and it's not prone for attacks and they also don't mind paying extra penny because you know it gives a longer value in a longer term. Maybe you might buy a couple of laptops in the same time you have this mac book.
Researcher: So openness is not must if you get what you actually want for example security and other things like flexibility and so on.
TS1: Openness, I don't really see that it will be 50-50. Because people also might not like when you know that something has room for breach or something has room for malicious things.
Researcher: If we look from your company development point of view your engineers would definitely like to have some open system because they get the patches done by someone else so they don't have to sit and fix the code.
TS1: When it comes to that business model, it's again a different story. Let's take the example of Linux. If I

can build on Linux it is good business wise and then we again lock it up on the top because it also depends upon who are my target clients. If I take debian or something similar, let it be I could get free patches and security updates, etc. but I make it locked here on the top and I am making something more like custom made solutions for my client and that's what I call being technology neutral. Okay I like the beauty of the Linux, there are a lot of platform which are open because you can bring in lots of features and if you can bring value on top of those, that's what the market is all about.
Researcher: Is it like forking out or just customizing Linux?
TS1: You can say forking out.
Researcher: So you take whatever was like a snapshot and then you start building on top of that.
TS1: We will be updating from time to time
Researcher: So you don't want to really fork out so it's more like customizing your
TS1: We will fork out but we will bring in the updates from time to time. If you totally fork out and don't have this update module it's probably not a good idea when it comes to technical.
Researcher: So if we conclude you are actually encouraging open solutions in IoT.
TS1: Yes. I would say that there are companies that are legacy which are really big and are too slow in delivering solutions or the possibility that we can do and who cares as long as I maintain the due diligence and all these things within the company and I have a bigger eco-system. We have being working with bigger players in the market because we have the bigger capabilities to bring in a short moment of time. Sometimes even better than the big players in our eco-system. That is how it should be. Hand shaking in way like a bit of open and semi way is always good and user friendly.
Researcher: Let's move on to the core of the interview. What are your views on security & privacy of IoT?
TS1: As of now I see that there are big breach possibilities as we speak right off. Because lot of the projects are being just like prototype level and they just thought without thinking the whole end to end but at the same time we are keeping in constitution that okay security is something that we have to add on. We'll be working with technique that is patented a few years back with our partners. That's how you connect all sensors in industries or how you work in buildings. So we still have kept room for security because that is the key that application really holds the automatically to the dashboard and you got to be really secure. Let's assume there are two industries and you are using the same structure and you shouldn't be showing the data from other industry here. We were working with one of the Linux based project, to be more specific, we were thinking what sort of security? We thought let's look at how Android was built from security perspective and so let's try to adapt the Android way. In this way you also get to know easy of doing secure thing. On top we also have some architect who look upon latest trends.
Researcher: You actually mentioned two things in your response: .1. Security is key thing and we have to think end-to-end security 2. At the same time you said, we think security as ad-on. Doesn't it contracting

each other.
TS1: Not contradicting. In the initial phases, when you have to show the capabilities and possibilities what you can do with IoT, at that level no one will have to really care about security.
Researcher: Okay so during prototyping phase one doesn't have to take care of security.
TS1: Of course we will still have in our agenda to be taken care. It's in the next coming version. So with that approach, if I can make a board or a big company realize, yes this looks really cool stuff on our product to be integrated and then they will see ok yes then they really start the whole process, like how you do at Sony or other companies with a bigger projects.
Researcher: When you say security as like ad-on can we actually roll out security after the product is like shipped?
TS1: I doubt because now a days we have devices that come with AES enabled hardware. So they have to come doing the hardware build as well. Of course there are frameworks we've been talking to some California based company and there's also one from Sweden that those are into security, especially how they can handle secure link and TLS and what sort of secure elements we can bring in. That would be an exception but it's not a normal way of doing things.
Researcher: What's your view on hardware security vs software security because you said now the chips are coming with AES modules enabled and what about if these chips were not there? Can we do justice with software level security?
TS1: It's more of am I in defense or defense applications or what vertical am I talking about. IoT is no exception for defense because they would like to grab with drones a lot of data now a days. It's also about the prices as well if you have to go for hardware enabled security you need to add an additional dollar or less to put on.
Researcher: So there are costs associated with an enabling security?
TS1: But there are also ways in order to tighten things on the other hand I don't say that it's not possible to jailbreak or like all these things there are room for. Why Google does pays to hack their site because they still wanted to keep room open. In a way they are using open systems. They make it open place hackers and we will pay you for what you find here.
Researcher: So it's like ever evolving topic.
TS1: I would see that as the ecosystem builds as the value of these devices in the real ecosystem increases the functional level of security also increase. It will evolve, why the frameworks or the open frameworks are or closed frameworks they are adding different elements. Even Linux is casting how to use this as a platform for IoT or what is the minimax Linux version that can be put on IoT device. One example would be if you have a sensor on a device or a machine that you put on so we also have an encrypted key that will identify the sensor itself.

Researcher: So it's very important to have this trust between the sensor and the data center.
TS1: Yes, it can be the sensor id that will be encoded and decoded on cloud.
Researcher: So is the data transfer between the sensor and the data module is also encrypted or it doesn't need to be and is just integrity protected.
TS1: For example, if you take in one of the applications would be applying HTTPS. So in a way yes, even though you're making like a packetized, you got that sort of certificate to be download.
Researcher: So we encrypt the whole channel instead of encrypting the data which is expensive like secure connection. Do you think we can actually use the existing security techniques or mechanisms which have on PC's and mobile devices on IoT?
TS1: To some extent of and I don't say that it is fully reusable as such, because of the capabilities of IoT devices is very small in terms of power on the device itself. It has to be low power and run on battery for a couple of years. We can get some inspiration from already exists on windows or even other OS like Android, etc... Obviously, all the innovations are coming from inspiration from what we already have because it's hard to come up with it totally new. If you talk about using bitcoin sort of technique for encrypting as well. I would say partly yes we can use but not exclusively no reporting everything here. It might be an expensive operation as well to just use as it is.
Researcher: So we can have the best security, but the battery will just last couple hours.
TS1: if I get data from some sensor every second of every minute or something that will be very expensive operation.
Researcher: We did not touch so much upon privacy part of the IoT. Do you see any privacy issues in using IoT devices?
TS1: Definitely yes. If you talk about the connected camera, why don't we have so many cameras in Sweden like Denmark? Because Sweden cares for privacy. The new law is also in place e.g. GDPR. I have not been digging deep into that, but these sort of changes are already happening. Privacy is very important because if you don't know what it means you will be scared to go out on the streets. Basically what is happening is that if you know that someone is trying to monitor on you on your behavior that's really crazy. If you know that there is some monitoring but that's more generic. If they want to know how many people come into this square during that part or the time during the day? So there are some behaviors that are being monitored but I think privacy is the important thing.
Researcher: So it's also important in your domain or your industry.
TS1: In a way yes. Do you use any techniques to address privacy? We're making machines or bringing lifeless things into life. What end clients says is that we want to have it house we don’t want to host it on cloud or something similar. They are afraid. Getting data from this also means that they are also getting access to their systems as well.

In one of the solution we are using in a way to making it secure that's also one way to make it privacy aware.
Researcher: if you want to have privacy you need to have security and which means there is no privacy without security?
TS1: Yes. That's how it is. We are working with some mass loaded project after summer and we are looking into what is the best way of doing privacy. So applications doesn't really need to handle privacy.
Researcher: Is it connected to the human aspect that is if there is human user than there is need to handle privacy?
TS1: A better user scenario is elderly care. In elderly care there are a lot of regulations. You can't have a camera to monitor elderly person. Even though it could be best effective but you can only hear some audio or noise level. We are also talking to a company that makes sensor that can sense elements based on the breath and what different parameter is of interest. So in that situation that will be personalized to human. So in that case it is OK if I want my grandparents to be monitored. I think it's a good way when you can't really physically be there but technology can fill the gap.
Researcher: How do you see the privacy issue when the users are not actually humans but it's the smart things? It could be like one thing interacting with the other things. It's like mesh of things. Do you see any privacy issues?
TS1: Yes, because you can backtrack. If you know that this camera or this particular sensor belongs to a particular person or region. So you're again hitting back to that particular location or the people that are connected to that location. So in that way, yes, they are also having some parameter connected to human as well.
Researcher: One way to implement security or protect the data for example is the traditional user name password and that doesn't work in IoT because if the system is implemented where the humans cannot reach then it's not possible. Do you see constraints in industrial applications? For example the sensor that you have in your hand it's impossible to have login kind of mechanics on each individual devices.
TS1: you're right, you can't have a login, but other hand you can have other techniques baby let's say you have a dashboard where you are controlling system. If my job is to be a maintenance manager for an industry or for a factory so someone got to take the responsibility for the whole factory, someone need to really take control. If there is breakdown someone needs to get access to know to stop the process or stop something. You have like fingerprint or even face recognition so as long as it's restricted to certain user scenarios it can be used these techniques as well.
Researcher: You do believe that we need to have ways to authorize things our users and then we need to have somehow trust management between these.

TS1: Not in all the scenarios.
Researcher: I mean when security is ON of course. If we need security then we need to think about these kind of aspects.
TS1: It will be again a bit of split. When you need security & privacy you got to be extra careful especially if you are let's say if you're selling a cancer treatment equipment so you don't want to connect it to like who is getting it. Then you can identify who has the cancer. He will still be able to use it in a certain way and in that situation the user experience, UX design will also come into picture because there is no one single way to solve it. Even if there are industrial applications you still got to see the user experience and how you actually can use or what is that you actually can put it forward. In most of the situations you are controlling things from the dashboard or the main application when you just hook on the device or a machine or any building or any place, we have even the hidden network behind the factories. For example this building they have control system, e.g. SCADA that is already in place at least in the western world.
Researcher: How does the dashboard knows that it's actually looking at the right devices because if somebody intrudes and put in there sensors they can dilute the data and it can get very different results.
TS1: For example, a lot of this bigger organizations they put a lot of emphasis on the budget for the security because something is beached, for example in some of our projects we have a very big penalty clauses if something breaches and that could really make a company bankrupt as well. The clauses are such strong. So you can imagine how important for them is to keep their data very secure.
Researcher: Do you go for security audits in this case?
TS1: I can give one example, it's been a year and half that we were being into one banking device or a banking application. In that scenario they had a very special requirement that there should be only one way communications they don't want to have both way communication because someone could hack it. They wanted additional encryption as well. So for those sort of things that we need to go for security audits.
Researcher: How about one of the important thing, i.e. software upgrades in IoT?
TS1: In one of the smaller device client was asking if we can have software upgrades. It was not recommended actually because of certain constraints on the technology itself. Technically it's possible but the problem is that we will drain out the battery. There is a need for software upgrade e.g. we have been working with some big clients where if they installed these devices remotely and they also don't want to send someone to just update the card. They want to have over the air upgrade.
Researcher: Is there any security without software upgrades?
TS1: As I said sometime the protocol itself is providing security in the transport layer or even on the data itself. In that way there is security.
Researcher: So basically the understanding is that there is no security if there is no software upgrade because if you know you implemented the best security today but after two years there will be so many

exploits available and if you don't patch it, then your devices can be compromised easily and that is what is actually happening with most of the IoT they bring the best devices in the world, very user friendly, very innovative? But then they don't even think of software upgrades, maintenance, and so on....
TS1. Why do you think so? Because I don't totally agree with you. Because the reason is that there is a plan for maintenance. When you are selling IoT devices installed, most of the important applications and scenarios, there is a plan for maintenance and sometimes it's easy to send updated h/w card replaced instead of repairing the devices or trying to reprogram it. It's more inexpensive to do that.
Researcher: Are you saying manual upgrades sometimes are a better option.
TS1: Manual upgrades are there at the same time there will be techniques that will take care of the, for example, let's say if this device is not very expensive, I would say, ok, every year I would just, change the device and just reconfigure it.
Researcher: It's not about upgrading the device it's about updating the software that you run on this device, so if you have a particular version of OS and that is compromised now so you need to provide a upgrade, you need to provide security patches otherwise your system is already compromised. Anybody can come and hack it. It's just matter of time that they realize it
TS1: Actually, I understand what you meant. Yes, upgrade will be entertained wherever our technology supports if technology doesn't support we can't do anything since the only ways to do it is manually.
Researcher: In some cases even the manual things are tricky because the sensors where they are implemented, the operational environments are so weird. It's quite expensive. This is a general view.
TS1: I follow you what you meant. That is true if I'm having my devices in oil rig which is running 24X7 and I can't really take it out and there are also two different types of obligation. One is primary, people are making devices for primary needs and they're also making for preventive predictive maintenance using IoT. There's also some reasons where they will have a fallback mechanism and where they actually have regional data using less precise sensor in inexpensive devices. So there are two ways of handling that situation, so in that situation, they there is a need for upgrades but at the same time not every situation will permit it, and either technological reason or some other reason. Anyway, most of these big installations they will have a schedule for maintenance. That schedule they will have to take care of that part. Either they do over the air or offline. That is also one design constraint because when you make a design you should also think fall back basically you can't just design which is forward looking. You should also think ok, what is the situation when I'm upgrading OS or security patch. Because the device will obviously not work and it should still be going smooth.
Researcher: So operating 24X7 is the most important thing than security?
TS1: I don't say that actually operating 24X7 it will go but as I said there is also a schedule for maintenance for all of these 24X7 as well because that is required to be able to the handle the process in a smooth way in

a longer period of time. If I have 2 or 3 plants that are running, I can make plant one to be under maintenance for certain days or certain weeks while I run the other one it's more like a typical project management. When it comes to device level upgrades wherever it's possible technically yes we will have to have that in place. It also matters at what rate, if you come and say look I don't have a budget but I still want it, then we will say OK please we can't do it. There are clients where they want to have all the fancy features but they don't want to pay the price and then we say ok we shall not work together.
Researcher: Do you say the cost is one of the thing which is driving the innovation in IoT to certain extent.
TS1: Yes, cost is obviously one thing. If you come and say I have only this much you will only get corresponding to what use spend.
Researcher: And then we are taking the risk of user privacy data
TS1: Definitely. That is the reason why we have certifying bodies and approval process. These bodies are controlling, e.g. we have a medical device in one of our project. If you need to go for FDA approval that is really you need to tell where you do even the single step for the whole product. It is really tricky one actually.
Researcher: So it depends on the domain in which IoT is implemented then certification is one of the way to ensure that we're delivering the right quality of product to the user.
TS1: Domain is very important and for the business critical, obviously even they know that they shouldn't worry about the price because they're getting more value than what they actually implement here. If you're going for a B2C and if you go and buy something from shell and companies at your own risk coming. But if you are buying some services or something than the risk is on who is providing the service. Obviously product ownership is always a big risk.
Researcher: Can we discuss standardization and open systems? Certification is one way to ensure quality and standardization is more about how to ensure interoperability in the same software used by most. The problems are shared basically. So do you see any opportunity in IoT, we should go for standardization of things or if we still keep things proprietary.
TS1: It is hard to standardize the whole IoT eco system because we're talking about multiple verticals in this case, and every verticals has its own limitations and its own requirements. So maybe a medical device might have one requirement and industrial equipment might have one other requirement. Medical applications for humans has many constraints. If it is machine then you are communicating with something which doesn't have a life. There are standardizations to some extent but it depends upon the technology and which vertical etc. e.g. BT 5 or BT there are no standardization body. Whoever is trying to do both certifications and standardizations they are controlling what is all. That itself is a big eco-system. If you take LoRa or cellular (GSM, etc.) who trying to control narrowband IoT and I don't think that you can bring one single way of doing all of these.

Researcher: So what you're saying is that we should look for standardization on the enabler technology and not on the IoT product as such?
TS1: I would say standardizations are there but the only thing that I would probably say is that they should be more security focused. If there is more security on this device yes obviously that's what we will need.
Researcher: If the enablers are already secure, if they already have secure solutions, then it will be very the easy to create IoT products?
TS1: They should start from the bottom layer because if the standardization bodies are not really taking care of it you would obviously not take over of it because you are just trying to patch it.
Researcher: So it should be bottom-up security and not top-down security approach.
TS1: We can add additional layer, but if you don't have basic layer secure then then you're really not secure and trying to pretend that you are secure.
Researcher: How would you actually implement security or privacy things in IoT solutions from development point of view during design/architecture aspect? As we saw during the interview you emphasized on the security you emphasized on open systems. Now if we have to think how we should do it, what are your suggestions?
Researcher: You want vendors to enable security so that is one of the key requirement.
TS1: When we can pick and choose the components in our design for the hardware perspective. We're also looking at what sort of support does these vendors are already offering? No a days all the cellular vendors are providing more or less different options for secure links. You can enable the multiple ways for handling data. What I see is that in bigger projects which we're dealing with in general for a big end applications (industrial processing, mining, marine). Not only having a lot of overhead by having security, but we also need to be optimal. The reasoning is that we have to, let's say you're in a marine ecosystem, the connectivity to the cloud is really limited because you don't have a cellular connection. So from the design prospective right from the sensing level or the communication platform level we got to think of what sort of security things that we can cooperate. At the same time on the application layer what add-on can we put in the design itself? Of course we can make a simple http application but is it really secure? Not really. Even though there is some limited security so still certificates exchanges or some sort of token exchange and sort of encryption. In one of the device where there is 128 bit encryption in order to unlock the device you need to have the code first. At the same the protocol itself is supporting some sort of transport layer, some sort of data overhead which you will be decrypting. In another application, sensor is given identifier maybe 64 or 128 bit identifier to be able to process the data on the clouds side to be able to see that you're getting data from a particular sensor.
Researcher: How about revocation of the data? E.g. blacklisting misbehaving node.
TS1: Now there are ways to do that but at the same time as I also mentioned if I'm making a modern

techniques or modern sensing element I shouldn't be affecting the process of the whole application. I should be adding value on top but if it fails I shouldn't stop anything else in the process. That's what we always see in the design. We have to sometimes be stand alone and if you are standing in the middle of some processors or middle of really execution time it is really not the best design. You always need to think of the fall back as well, what if this fails to work? It should still work. In terms of not this function may be you would just stop getting data from this but you should get a notification and you should identify that and then you can do something about it.
Researcher: Do you want to make a final concluding statement to the audience?
TS1: In IoT we have vast opportunities and vast use cases. IoT without security I do not believe in. Security & privacy are key element for IoT to fly. IoT is just a tool or enabler. At the end based on the applications and user you will define what level of security & privacy is needed. So that is all connected to what eco-system we are in what application and which markets European Union might have a different regulations than US, or may be Asian markets has different. You also need to look at which region that we are in and what verticals and what applications and which business segmentation, i.e. are we in aerospace or are we in Marine etc... So without security and privacy, I wouldn't see that IoT would at all fly. I believe in data and security, these are the two things that will only live longer in terms of handling the whole ecosystem together data is nothing less than diamonds. If you can't protect this data with secure link or security you are lost.
Researcher: Thank you so much.
TS1: Thank you.

Appendix D: Interview of SN1

Researcher: The protocol is like I will record the interview. I'll make a transcription and I will send it to you. If you want to, like, remove anything, any parts off it we can do that, and once you give, ok, I'll try to use that transcript as an appendix in my report, and we won't identify like individuals, but more as a group, what is the thinking or their opinions on certain aspect? And then publish it in Malmö University.
Researcher: Let's start with, like the first interview question that I have and that's about your role and how do you contribute to IoT?
SN1: Yeah, my role. I'm XXX of sensitive AB. I'm also to a very large extent defining on a high level the IoT products that we are doing in sensitive and that might be devices, or it can be the platform, or even sometimes services.
Researcher: can you describe more about like the products Details like technology wise.
SN1: We are developing sensors for smart home and smart building. We are selling them under the brand name strips. And we have some sensors using the communication technology Zeewave we also have ZigBee. There are different variants in the market for different functions. We call them strips guard, which is a magnet sensor for the doors and windows. We have strips comfort, which is a sensor measuring temperature and ambient light. And then we have strips drop, which is mainly a water leakage detector, that also measuring temperature and the ambient light. Those are the sensors that we have in the market today, then we have a number in the labs.
Researcher: You do full stack or you take operating system and customize it?
SN1: In this case, I'm not sure if you talk about full stack when you talk about the embedded software. So in those cases, the sensors are rather fundamental. Processors are old fashioned Microcontrollers, software is written in c, we are utilizing reference code but rewriting to a very large extent.
Researcher: I see and do you use open-source for this matter.
SN1: No. We foresee what sensors on the company behind these is the sigma design that was just acquired by silabs and sigma design that is offering the protocol stacks and the reference code. In the terms off the ZigBee we have got the whole reference code and the protocol stacks from Silabs.
Researcher: Great. Thank you. So let's move on towards IoT. What exactly IoT, internet of things mean to you.
SN1: It was a very narrow question... laughter...
Researcher: So going from like specific of sensitive to generalize this. Then we can build upon this open source.
SN1: For me IoT is all about connecting devices to internet which is very different from connecting devices to a remote controller which is basically how most IoT devices work today. So maybe we should

talk about IoT 2.0. To me it's all about creating a world of connected things that can be utilized by lots of services and lots of people some connected devices would be very private very personal a very dedicated for a specific purpose what others might be used by many services and people.
Researcher: When you say connected it has to be with internet that there is no IoT without internet
SN1: Well internet of course is not going to be there forever either it will be replaced by something else, right?
Researcher: Okay, yeah
SN1: But IoT, for me, means that it's connected to a world where you have users and services in a mishmash, running on some kind of system compared to connecting it to BBS which was very dedicated vertical.
Researcher: Yeah, that makes sense. And when you say connected, is it like the smart things that they call or something else that connects to the public network? So, what I'm trying to ask is that is it a direct connection from the smart things or internet of things, to the public network? Or is it like the intermediate thing like router which then connects to the public network?
SN1: To me that doesn't matter. Whatever way you take to get out there doesn't matter? **Researcher**: Ok, well, that's a very beautiful answer, so there's like some public network on the other side, and then what happened inside is not so important. And can we discuss more about the smart things in this IoT context like what are its properties or features and how do you perceive those? Because I have been like interviewing and researching and it's like, very different views on these aspects.
SN1: Yeah, I also have very clear views. Early stage connected things to me. Basically, you had hardware providers, product providers that put typically have a remote control, a little plastic thing that you call the remote controller and you used IRDA or wireless to connect, right? Once you take this product, whatever that product would be and connect it to a remote controller in your mobile phone instead, exactly the same functionality. Then suddenly people started to call it a smart product, which for me, doesn't make sense because it's the same product as before you had just moved you remote controller from a dedicated piece of plastic to a mobile phone piece of plastic, so I would not call that smart product. For me and smart products is all about actually utilizing internet. Putting the smart products into relationships with loads of other smart products and enabling loads of smart services to actually do something with it.
Researcher: That's a very nice comparison.
SN1: I'm comparing this with the brain every now and then and the human body. If you have a dedicated brain for every muscle in your body, that muscle wouldn't be very smart. Now you don't. You have a much more complex system, right?
Researcher: So for you, communication is like the key in this whole aspect.
SN1: In your body again you have your central brain but you also have a lot of distributed small brains like.

Like you have muscle memory I am not sure about the terminology here but the muscle in itself doesn't need to get the response from the brain sometimes. If you get burned the muscle directs immediately. It's kind of distributed smartness, and the muscle is able to connect to millions of muscles and sensors and everything in your body and make the smartest thing out of that.
Researcher: okay. I'm satisfied here with understanding off IoT. Let's move on to the constraints that this whole ecosystem puts on different components of the eco-system. So can we discuss little bit about that and if you face any constraints and how do you overcome those.
SN1: Constraints. The hallmark today is very vertical. 99.9% of all supplier of smart products they package complete vertical solution to the consumer and sell it. The consumer the ends up with a number of vertical solutions. And realizing that they cannot be connected or at least it's very cumbersome to connect them. In my world, that is one of the main reasons why we still talk about ideas, they talk about smart homes, but in practice it is still not volume markets.
Researcher: Is it interoperability?
SN1: it's very much interoperability, but it's also about actually being able to connect multiple services to same services. Even if it was compatible, that would not mean that it's not vertical. We need to move from the vertical business models to much more horizontal business models.
Researcher: Is it more about opening up the API's?
SN1: For example, again let's go back to the internet. Internet is very horizontal because you can connect, everyone can connect. Hardware and give it an IP address and give access to others, right. Anyone can make web service and allow other people to use that and connect that web service to this device that was connected through IP. If you get the access rights. To me, that is the horizontal business model. Before that, before internet, we connected to BBS and the BBS provider gave you a telephone number. You can call the telephone number with your own modem and that became then kind of vertical. So different BBS providers have different phone numbers that you can connect to. And for different services you needed to dial into different BBS's. Same thing with mobile phones, go back to the early stage of WAP and then mobile browsers. We had in Japan IMOD. IMOD again was not to the internet that was a vertical. IMOD try to lock in the use to their own vertical. You change mobile phone to orange and you got an orange instead. Those who are not in my world smart phones. It became smart phones when we opened up and you enable smart phone users to use not only IMOD and DOCOMO's flavor of services but anything.
Researcher: So basically what you're saying is that if I go to a shop buy some product and then I should be able to choose which service I want to use with that product
SN1: The hard connection between hardware and services is. I have a good picture from vison Mobile. Do you know vision mobile?
Researcher: No.

SN1. Okay. Vision mobile is a strategy and analyst company that are doing a lot of market research and so forth and they are quite often in Lund because there is a sort of connections between Vision mobile and some of the guys over Sony. I have a very good picture showing dual helix. You basically go back and forth in different technology fields between vertical and horizontal models. While you are always in emerging markets, emerging products, you need to start vertically because the pioneers they need to do everything themselves. So they package the complete solution but once the market matures, they start to have different companies, different suppliers going in and taking different fields in the total market. Sony mobile phone business for example you have the Qualcomm taking the chip sets you have the Google taking the software, you have millions of apps suppliers taking that applications. And suddenly you have created horizontal business model. IoT is still in the vertical phase.
Researcher: How can we overcome these problem of vertical to horizontal model?
SN1: It's the maturity. It's about compatibility and it's about different companies specializing in in different segments in horizontal model. But as long as everyone is doing the complete vertical it doesn't happen. If you look at mobile phones when did it happened? It happened when google launched android.
Researcher: yeah, but android was such an open system even though it's controlled by google but still its lots of openness in that,
SN1: Yeah, Android enables horizontal architecture because it's a middleware, where you have apps on top. Where we have the possibility to do apps with cloud based and a lot of services in the clouds. Where we have device and you have the possibility to connect hardware underneath. And the possibility to connect hardware not only inside the phone but using the usb outside the phone as well. Android is fundamental to create the horizontal model.
Researcher: Are you saying, like we're missing some kind of middleware operating system for IoT.
SN1: That's my view. Definitely.
Researcher: Does it mean its missing standardization of these operating systems that are available and different software that we have.
SN1: I do not even see that there is any trial to make such standardization.
Researcher: But do you think it's going to help address the problem off this Vertical vs Horizontal?
SN1: Let's, see. Half of what sensitive is doing is creating such a platform? That's what we do.
Researcher: The next question is more about the openness in the IoT systems. I will just connected it to the conversation we are having. So when you say sensitive is already doing this horizontal model, do you think it is just enough, like sensitive is doing that or you think it's important to involve the whole community like the IoT community in building up something like that more like Kernel.org.
SN1: I see others doing parts of this as well. I see both Google assistant and Amazon's Alexa, also components in a horizontal business model. To some extent, you can see Microsoft and IBM, even though

they are as more behaving as Symbian used to do once upon a time for mobile phones which is creating a plastic bag with all the software components you need to build, your own vertical solution. That still taking a position in horizontal model where there are supplier to IoT vendors. The position IBM and Microsoft take is more to support the vertical vendors and creating horizontal business model.
Researcher: So how do you think openness can affect the internet of things? There are various theoretical models around which advocates properties or characteristics like flexibility, extensibility and customizability of the open system. Do you think openness is about flexibility, customizability and extensibility? How do you think openness is actually going to affect IoT? I think you partially answered my question, but it will be nice if you can elaborate more on this.
SN1: when I hear flexibility and things that directs me to what Microsoft IBM is doing with their blue mix and nature. I'm more looking at the Android model where you have very good managed environment API for android, for app developers, app developers know exactly how the API and the language and the support they need to do in order to make and app. They know how to get to the app approved by android or google and they know how to bring it out to the market and they know how to monetize on it. Android is not very flexible, right? It's a very quiet rigid API. Android as such is not possible to customize you can build your own UI on top, but there is a very strong directive from google that you should not customize too much right. And in fact there's a huge penalty if you start customizing it too much because you will have difficulties to do upgrades so it's not very customizable either. Yeah from that point of view, I think Android works well because you have the possibility to add millions of apps. You have the possibility to have many apps so they're using the hardware at the same time so it's a simultaneously. You have the possibility to add cloud based services, you have the possibility to extend the hardware you know with the USB and even some modular designs for some Phones. So Extensibility scores high but the two first no.
Researcher: And what does that mean for IoT if Android does have these properties? What does it mean for us? Like for sensitive? Are you missing such a platform?
SN1: Yes, we are. I am missing such a platform. We first started working with IoT towards multi apartment buildings. And building owners are real estate companies. They were looking for a standardized interface to the digital building so they can connect multiple services to the digital building that does not exist or did not exist but that that is what we're developing. The whole point is that it should be almost as easy to develop services for building as it is to development apps for mobile phones.
Researcher: Let's move on to the actual agenda which is security, and privacy. I usually spend a lot of time on understanding the whole concept and then slowly going on security and privacy. What are you of your views about security of internet of things and let's club it with privacy as well.
SN1: It is a broad question.

Researcher: It's like two questions we can take hand in hand.
SN1: what I think about security?
Researcher: security & privacy for you for IoT. Let's go in details on answers to this.
SN1: what is it? It's a huge challenge. The ability to secure user integrity while at the same time building an open system that really can utilizes the power off all the data that you can get from large smart systems. When you look at it very quickly it sounds impossible sounds like very contradictory but in fact it's again going back to Android in fact it's exactly same contradiction as you have in the smart phone where you have the open API developed by android and at the same time you have millions of app developers that no one can have 100% control over exactly what they do. But at the same time you have apps for banking and personal data and it seems to work okay. And people trusted even if it's some flaws here and there.
Researcher: So you mentioned the user integrity and the trust management.
SN1: yeah, there are loads of those, like integrity of you as a person, integrity of your data, in case it's devices that are used by many integrity of the data which means is it the correct data?, Has anyone altered the data ? Has anyone actually put in a new data stream pretending to be someone else? How can we trust this sensor or to be the correct sensor? How can we trust this service provider to be the service provider that you think you're sharing your data with? If you share your data with your neighbor, how do you know that your neighbor doesn't share that data with someone else? You store the data your data in different places, how do you know that that storage is safe? How do you know someone doesn't sell that? DOS attacks, DDOS attacks, all the financial transactions in there.
Researcher: So is it more about how user can allow data to be reused, use for their benefit and even the control over that data how it's used. If it can be used and how it should be used but this seems pretty tricky?
SN1: It is tricky.
Researcher: It's like lending permissions to someone. It is like blockchain,
SN1: Yes you can probably use blockchain.
Researcher: You said like I gave this data to the neighbor and then if neighbor can do something with it or not. It's like you are lending your permission to someone.
SN1: To some extent that part is not solved as of today. It's the same when you put up your picture on the internet, how you know that that picture do not hacked or copied.
Researcher: But you don't care if you put it on internet its thumb rule that whatever is on internet is public. You should not put things that you don't want to be on internet and that's why people go for a closed system, sometimes, but that trend is like changing I mean they're opening up a lot at the same time they're talking about GDPR.
SN1: You have that contradiction. Exactly the same contradiction you have in IoT. You put up sensors in your building and if you share that sensor with just one service provider, then you need to put your trust

into that service provider. Or you need to make a contract and agreement with him and then trust that they follows agreements. If you share your data with private persons then you need to put your trust into what those private persons do.
Researcher: So trust is the key here.
SN1: Partly trust, partly legal agreements and partly knowing what to do and knowing what to share. Exactly as with internet.
Researcher: Do you think people are skeptical about misuse of their data?
SN1: It also depends what data it is. If you have a thermometer on the roof of your house, why would you care? If you have motion sensor in your shower might be a little bit more interesting. If you have a video camera in your shower, yeah, then you care. But then again, you need to know what you're doing. Systems that provides this needs to be easy to use to give you an understanding of what you are doing.
Researcher: So if we talk about security, so security should be able to scale up depending on what kind of data it is. It could be like no security at all because it's not needed but it can scale up to like the top most like cyber security.
SN1: Yes.
Researcher: And that's not possible in IoT at the current moment.
SN1: No. To some extent it's possible in a completely vertical closed systems. But there is no tools, no means for this in any open system. There is no standardization for how to handle this.
Researcher: But what do we need one solution fits all kind of thing or it can still be like fragmented because the use cases are so varying.
SN1: How would internet work if internet were fragmented into different segments like industry and school and company and private and sex internet? That would not work, would it?
Researcher: But internet is more like a backbone and internet is also standardized and that's like the other thing, that's one of the key thing. As soon as it became little popular it was standardized immediately.
SN1: And before that you had BBS and they were fractioned.
Researcher: Is IoT about one solution fits all like Android it works for 70-90% of all the mobile handsets in the world. Is that something we really are looking for?
SN1: Would it ever happen or may be probably not. Will it be good...? I think so.
SN1: I don't know. Android work pretty well even if you have how many different ready protocols do you have in the mobile phones now. It is not the number of protocols we are talking about.
Researcher: I see you point. I think the middleware is the key, that's what we are missing.
SN1: The Android in the middle that connects the dots with the lines.
Researcher: Exactly OK. If we talk about security again so how that does connects to middleware things. Should security be built into the middleware or it doesn't matter where it is

SN1: I think. No I'm very much colored by what we're doing. But we are basically following the principal of Android and mobile phones. Communication protocols from the phone outside whether that is GSM or 5G or Bluetooth or Wi-Fi, you always have security on the protocol level. Right? Perhaps you have the certifications, you have the API, user give access to the app to certain devices and that's probably more what I don't even know about. Every app have his own credentials, every app can store his own data connected to the service, you can have multiple users in the phone and every user has its own credentials. Every user than have access to their own file manager, mail, folders etc. What else? There is probably a lot more.
Researcher: But this particular scenario is not going to work on IoT. Like multiple users
SN1: Why not?
Researcher: You don't really like log in into these kind of sensor. It just collects data from whoever it is, doesn't really care with logging thing. In most of the use case.
SN1: Could do
Researcher: So what is your perspective? It's not exactly the same use cases because in IoT it's very varying use cases that we talk about and its different companies doing different kind of things. How can they take like the similar solution?
SN1: If you are a middle ware and if you do as Android do, you connect all the technology in the phone. If you connect all the technology in a building to plug to middle ware platform and then you have Access management in the platform. So it's not that you're asking permission from the sensor so that you have 10 different users on that sensor, but you don't have ten different users on the GPS module either.
Researcher: So where do you think this middle ware will be running? Is it like on cloud or hub or...?
SN1: Doesn't matter.
Researcher: It doesn't matter even because there are certain constraints on certain devices and components.
SN1: Technology wise it can be in the cloud, it can be locally in a building or it can be in hybrid.
Researcher: So from the user point of view it doesn't matter where it runs but based on what technology is available
SN1: From the user point of view it matters. Obviously, if you have it in the clouds you have constraints of cloud. If IP goes down you cannot access it anymore. Same thing with the mains if 220V goes down it doesn't work anymore. Also turnaround time it's not responsive. If it's only in the building you can't have the remote access, with a hybrid it gets much more complicated.
Researcher: So why do you think like security privacy is so critical in IoT context? Why should it be there? In what phase do you think we should think about security and privacy? What phase of software development or product development we have to think about it.
SN1: Have you ever tried to put in security after software product was ready.

Researcher: I have seen companies doing that. They failed terribly. They claim like they are security experts but they miss the main point.
SN1: It doesn't work, you need to build architecture for security, right?
Researcher: Okay. So you is it during the designing, architectural phase or it's even before that when the concept has arrived when you actually start thinking about how to handle. Before answering this it's more about the previous question, i.e. why do you think it's critical to think about security and privacy?
SN1: Well, maybe I should start by going back to the current system. I can go back to BBS. Maybe even before that, let's start with BBS. With all BBS you had an encrypted line between your modem and BBS that was on the different service somewhere. BBS in itself could have been encrypted hard disk. If you were really concerned, you could have your own copper cable between the BBS and your own computer. In theory you could claim that the security is hundred percent because you have control over that cable. If anyone anyway would get access to the cable it's still encrypted and you have also your own server. BBS service is locked into your office and if anyone in the way get access to the server, it is still encrypted. It's easy to argue that you have the highest possible security. Once you are out on internet, things became much more complicated because everyone have access to the internet. But we have still learned how to create different security measures, security tools, security protocols, and security whatever. Now I forgot your question... laughter
Researcher: It was about the criticality of security in the early context, why we should think about it and then we will come to the phase where we should start thinking about security.
SN1: To be to be fair, internet from start did not had much of security. Then there were bad guys that took advantage of poor security. And then step by step you started to build the security on the internet. It seemed to have worked to some extent. Is it the perfect security architecture or should you have done internet in a different way? If you start it now, what do you think?
Researcher: Yeah, it's one of the question everybody is asking like, should we reuse internet? Or are we going towards something completely new which should be built for IoT. There's no, answer me, It's a very good research questions I would say.
SN1: When you set up an architecture, any kind of architectural where you have inputs and outputs and multiple weak points and multiple API's and so forth. It can easily identify the weak spots from security point you?
Researcher: So are you suggesting doing threat analysis immediately after requirements
SN1: Isn't that what you do?
Researcher: It depends and is so different from different organizations. Many of them, they don't even know what threat modeling is and some don't even care, they just go and buy solutions because somebody claims like they have the best security, so they just buy it. That is trends within IoT startup companies, I

mean, they have absolutely no clue about what security is? They don't even care about it and the most important factor is like time to market and how they can go down on the cost so they can compromise on like hardware security versus software security and so on. So it's a very different view, but I was trying to get your opinion. So if I understand you correctly, like security is one of the critical thing that we have to start thinking from very early phase and then built into the product rather than thinking retroactively.
SN1: So that's the way I see it. In practice this kind of process is iterative. You have to align with the resource you have and you need to align with your customer projects and so forth. In practice, you build solutions towards your customer requirements. And in parallel with that, you put your effort into building architecture in the correct way and making sure that you have the correct security. In times you have to put all your resources into meeting customer requirements. And then you need to back off because you need to renovate both architecture and security.
Researcher: Is security more about the tools and mechanisms that we have or it's more about the process and mindset
SN1: That is a good question. I don't think you can say either or you need to say all.
Researcher: End goal is to protect the software and the bugs could come from any parts. It's not just about storing the credentials.
SN1: yeah, you're right. Security problems can occur also from week security in your development tools. If you have done everything perfecting in your production code, if someone gets access to your tool environments to deploy a new software which they've changed and it doesn't matter that the whole production code was perfect.
Researcher: Are you talking about end to end security? If there is a security it has to be throughout the chain.
SN1: That is obviously one of the challenges when you start talking about horizontal model because you have at the bottom you have devices that are off the shelf devices that someone have developed. How can secure that also are perfect. You can't and then you have gateways assuming those are also off the shelf. Again very hard to be 100% sure. Then you have the middle-ware where you might have third party suppliers in the middle ware. Again if you compare with your pc , you have the Microsoft OS but you probably have plugins from different suppliers as well that you need to trust or not and then on top of that you have the apps or the web services that you need to trust. So if you look at what we are doing, we are taking the concept of android meaning that we are using certificates for services and you get a certificate after we have verified that service works and then starts working but if we start to get reports if something doesn't work, then we can take down the certificate and the service provider doesn't work anymore.
Researcher: And that you can revoke on live devices?
SN1: We don't have live devices like that.

Researcher: I mean the products that are already in the market or
SN1: The products are cloud or hybrid. Every service needs to have a valid certificate of, a valid token in the cloud. It is different from mobile phones that can be disconnected from the clouds.
Researcher: You have taken out most of the security from the hardware to the cloud, access control.
SN1: Security between device and gateway is basically managed by each protocols and that we need to trust.
Researcher: They're pretty much standardized protocols.
SN1: It's getting there. It's not really that easy. You have Wi-Fi IoT devices and they define their own protocols.
Researcher: What are the challenges you see in using the existing security tools, techniques or mechanisms in your kind of products. You can just take it from the pc world and put it on IoT and it works?
SN1: They are not that different. You have loads of security tools, code, used in the internet world today. You have secure protocols, you have encrypted protocols. You have the possibility to encrypt data and store. Our challenge is more that we have to be compatible with a lot of different protocols and techniques. I think how we combine and put together and security holes occurs because we're trying to connect too many things and in the connections there might happen things. Another challenge in IoT, very likely is, the amount of devices and the amount of suppliers of devices.
Researcher: How hard this amount of devices is a challenge? Can you elaborate on that? I read this from literature a lot, but it's hard to grasp that concept.
SN1: Why it becomes a challenge. It becomes a challenge because somebody needs to manage those devices. Again, go back to **what is security?** Part of security is to know that the data is correct. How do I trust that this thermometer is actually measuring the correct temperature, How do I know that it's placed in a position where it gives the proper value. How do I know that someone is not manipulating.
Researcher: If we have created a technique to establish trust with one device can't we re-apply the same on all the devices that exists.
SN1: Well, I guess so if it's only about technology but it's about people. e.g. let's assume you have a city and let's assume that city decides to have air pollution sensors all over the city because I would like to control. Let's assume that traffic speed and how you actually lead the traffic through the city is based upon this data. That could mean for example, if you have a very traffic in an area with a lot of traffic that a quite polluted. Then what happens is if someone realizes and also realize that if he manipulates the data from a couple of sensors that would enable him to use his favorite road. While if he do not manipulate data than the traffic is led around the city instead that he needs to travel much longer. That's typically a case where someone would like to manipulate data.

Researcher: I am actually out of questions for now. But is there any last statement that you want to make to like the internet of things community developers, academic researchers that you think should really think of or do.
SN1: What I think. I think the whole, I think the whole IoT world right now is putting way too much focus on compatibility between standards which is possible to overcome and way too little effort into figuring out how to make horizontal IoT world instead of the verticals.
Researcher: It was really interesting talking to you and it was different perspective I got compared to other interviews I had. Thanks a lot for having me in your office.
SN1: Thank you.

Appendix E: Interview of AX1

AX1: There's a big lack of research done in what actually works from a security perspective.
Researcher: Exactly and that's one of the findings I had in my literature review, they talk a lot about security, but they don't really talk about what is needed.
AX1: Yeah, and even if you talk about what's needed very few know the actually effect.
Researcher: yeah, that's even true, and no one talks about the general awareness part. It is so important unless you even know why you should have security what's the point in that actually implementing the security so these guys, they go for implementing it, but then they do a quick solution because they want to make dollars immediately and you never know.
AX1: So please, we will not have that much time.
Researcher: so exactly I'll have, like, still, I'll have some basic questions, but we can do it quick, so I'll start with, like, what? Your job role and how do you contribute to IoT as such?
AX1: Yes, so my job role is I'm a security coach, so basically ah, what I do is I help R&D organization develop secure software, and since axis is doing, IoT products that's, how I contribute.
Researcher: That's a big contribution and what does internet of things actually means to you.
AX1: Yeah. That's. A tricky thing. So for me, personally, I think it's an it's a strange term because I see it more like it basically means that more software is internet connected. I don't focus so much on the packaging of the product or what the product does. It's, just there is more software on the internet. That's how I see it.
Researcher: So how do you see the device part of it or the things part of the IoT.
AX1: Yeah, but that's where I cheat because I don't think it over it as much as things as I think of it as a software.
Researcher: Okay, so software is the key.
AX1: software is the key, it just happens to go in other boxes these days.
Researcher: When you say software is it like the software on the things or its software in somewhere in between communication or it's on the cloud? Or It's, everywhere
AX1: It's everywhere. But I think that's one of the things with internet of things is that the things rarely act on their own. They need some back end. So it becomes this it's a thing it's a connection and its backend.
Researcher: so is backend like part of the internet of things or it's, more like a dependency.
AX1: Yeah, so in my personal perspective, because I really like the system approach, I don't see a difference between the various parts in the in the system, they just they work together, so whatever we do from a security perspective, we do the same thing on the product as we do on the back end it's just software in one abstraction,

Researcher. And is it ok if I ask you why you do like the same things on both?
AX1: Yeah, and when I say the same things is because we're really focusing on teaching, the teams how to develop secure enough software for their environment, so we're not focusing on technical solutions, so we're not focusing on you should use TLS or you should use two factor authentication or this crypto we're teaching them how to think about security in what they're developing, and that thinking can be the same. Whether you work on an embedded product or a cloud service
Researcher: And that will ensure that it is end to end secure,
AX1: it ensures it's end to end secure, even if the technical solutions chosen by the teams are super different.
Researcher. O that makes sense. The next question is like a little off track, like it is more about the properties off, the smart things and the immediate next question is actually the constraints that you've seen in IoT, and maybe we can take them together.
AX1: So from an Axis perspective, it's a kind of a strange situation because, uh, this company has been doing in actually it's in a cultural, corporate dna to do internet of things, things we were doing that before it existed, because basically what we do best is we put the Ethernet cables in stuff, so we have been, like a company connecting stuff to the internet all along. That's one piece and the other piece is that we've been doing open source and Linux for a long, long time, so it means it means that we have been doing we've been we've had actually pretty powerful hardware all along said we don't come from, like, the really know and micro like sensor where actually much richer products, which means that there haven't been that much constraints from a technical perspective. So it's kind of weird, I mean, do you think about the internet of things? And then you think immediately of constraints, but there hasn't been that much constraints from what you can do with the hardware.
Researcher: And this was specific to the axis products?
AX1: Yeah, I think I was trying to put us in context, we're not really felt the pain off really small products because we're not in that segment.
Researcher: I can twist the question because now you say like it's not much constraints in axis kind of products when it comes to IoT, what does it actually mean in reality so if one had like constrained environment, how does it impact security and there's no constraints how the life is easy.
AX1: so basically all it means is that with no constraints you can chose much stronger e.g. cipher suites for TLS. That's like the immediate impacts. If you don't have any constraints, you can pick the best stuff.
Researcher: when you say best stuff like the already existing
AX1: already existing so best basically a standard algorithms its good key lengths and you don't have to think about much. But if you start to get constrained you need to become a little bit innovative on the crypto side and that's difficult and it's dangerous.

Researcher: Yeah. So if I rephrase it it's more or less like you will be solving the existing problems rather than solving the new problems which works orderly?
AX1: Yes and that's a good thing from security?
Researcher: Yeah, definitely., it is the next question we're actually already on midway off interview but the other ones might be more detailed, so this one is specific to what you said about Linux and open source so how does this openness in IoT or how does openness affect IoT and the traits that is like evident from academics or literature is like the openness usually have three properties like flexibility, extensibility and customizability. Well how do you see like open is in context of like IoT.
AX1: yes so for us again in the axis context one of the major property on how we have set up our business is that we up until now we have been very much a hardware company and we focused on just doing the cameras and we really wanted partners and ecosystem to do the backend services and whatever extra features needed so it means that we actually have a, uh very large ecosystems of partners and developers that actually develop additional software outside of the camera as well as inside the camera so for us that has been a fundamental way of actually reaching the markets we have reached. So actually we have used that. So axis is we're not selling directly to any customer but we are selling through partners always and those partners often add stuff to our products.
Researcher: And by stuff you mean feature
AX1: features. So basically we have our own I don't want to call it app store but basically our own framework for adding software to the cameras.
Researcher. Is access adding the security like what is it called provisioning the security out of the box or its partners who are responsible for enabling the security?
AX1: yeah so that is the tricky thing so again this is like it has to be taken into historical context so the video surveillance industry a long time ago it was an analog industry like fifteen years ago so they were like special cables so you didn't need security because everything was analog there was no software security, there was no software running in any product. We're just like cables to cameras to monitors. Basically axis changed it to a digital. We basically transform the market into going over IP. but it was still on close networks for a long, long time it was on close network so we basically relied on the customers hardening their infrastructure and putting our cameras or products into that hardened infrastructure.
AX1: So it was basically the responsibility of the customers but it is changing because a lot of customers are moving towards a situation where they for economic reasons wants to put these devices under normal network. It's too expensive to have 2 networks.
Researcher: Especially like in home security they have to rely on public networks.
AX1: so that's a really major trend that everything is moving towards public networks for basically for cost reasons and then all of a sudden everything is exposed and we will have to take larger responsibility for

securing our customers because not everybody can secure themselves.
Researcher: yeah so how do you see, like, Linux or open source operating system contributing to this this whole story.
AX1: so Linux and open sources contributed basically, in the perspective of the, um, the fact it has been quite easy to create these ecosystems, because if you can develop for Linux, you can develop for axis camera. And we haven't had to invest too much in building basic technologies like open SSL and stuff because we could just picked it up. So those are major benefits. But over time there is a, I don't want to call it drawback, but there's a challenge if you use a lot of open source components, uh, you need to put some sort of vetting mechanism in place to figure out whether they are secure or not, um. No, this is my personal theory or opinion. I mean, if you go back a long time open source was better than a close source because people were paying more attention. So basically since developers knew that somebody would be looking at their code they actually did a better job. Yeah, but now a days. I think that it's not it's, not obvious that's too coward, I'm actually what I'm becoming more and more convinced of is that, uh, modern open source projects are actually less secure than what professional companies can do, because it's actually really hard to make secure software you need to invest in doing that. And if you do that on like a two, three person hobby project, you can't compete with the professional team or people using tools, and processes and what not.
Researcher: [00:12:16] but if the community is, like, really big for example, kernel.org, so many contributors.
AX1: Some open source projects can't compete, but I think in, uh, in the population of opens source projects, I think it's actually a few that are that good. So the best ones are probably better than what you can do, not because they have better processes, but because they attract better people
Researcher: Does it mean, like it's kind of standardization of open source in a way. You use more mature communities SW.
AX1: I wish we could, but that's actually not the trend, so we're using more and more stuff and that basically means that we're using more and more stuff from smaller and smaller communities that are actually weaker and weaker in security. So that's, the worrying trend. So the Linux kernel and those big mature projects they are safe because they have smart guys. But there is just so many smart guys and girls on this planet, so a lot of software is actually developed by not so smart people. Yeah, yeah, that's a challenge.
Researcher: But do you recommend using Linux or any other open source on other IoT products, and not just axis products?
AX1: Yeah, and I'm now this. You have to consider alternative. So if you want to be more secure in using open source products, you actually have to be smarter than those guys. And most often you're not.

Researcher: How do you ensure it's more secure? Is there some kind of verification, like formal verification?
AX1: There is not that that's actually the thing. At axis we are around one thousand developers. So making sure that we develop good stuff on our own is a huge task but we developed like twenty percent of the code that goes into product. so if we would spend the same amount of energy in securing the other eighty percent of the code going into the project, we would I mean we can't afford doing that from a security perspective that would be a huge security team vetting other people's code during formal verification and using tools and what not that not that would be like it's not economical .So what we're doing right now work the best we can do right now is to look at historical evidence have they had many incidents basically. It's a really weak measurement but that's what we have.
Researcher: ok, so basically what you're recommending is like if it is too expensive take the risk and then see how it behaves and then be ready for patching it
AX1: Yes, Yes, that's basically where you end up.
Researcher: So that's what you get when you buy open source.
AX1: absolutely I mean there is no other I mean but that's the game we play.
Researcher: But can we apply like Linux and open source in other IoT products where the system itself is like so constrained in resources.
AX1: that could be a problem that could be a problem.
Researcher: And do you do you see anything like the alternative?
AX1: And in that case that we haven't had to consider that at all? So we haven't even asked ourselves that question. Yes, it's a luxury position. **But again, I mean, the key point I'm trying to make is that it's, not the technology that makes the thing secure. It's actually your development developer community that makes the things secure.** So if we were to let any of the open source projects, we will probably not go look at the code. First, we will go and talk to the guys, so the ideal case would be to talk to them on ask, how do you how do you do when you, you develop secure code?
Researcher: So now I'm late getting into the next questions. So what exactly is the security? The question was more like, what are your views on security of internet of things. But let's start with what exactly is the security when we say security? What exactly it means?
AX1: So in this context, securities related to, ah, security bugs and security bugs are basically bugs that have two special properties. One property is that there was an active attacker using this bug. So it's not like a random event. There is an active attacker, and you're using the body to commit something that this malicious, with malicious intent. Stuff that happens randomly, I don't think about that as security problems. There needs to be an active attack doing something with intent.
Researcher: I see, and those things could be caught in code review.

AX1: Yeah, and basically a tricky thing with this is that. So what we are working with this is that to catch these security bugs, First of all, there is lots of them in all software. They're so actually problem is not finding individual security bugs. The problem is to find enough of them with reasonable, economical effort. I mean, they're basically so many so you can never find them all, and you can get totally lost on finding some class of them. But finding the once you need to find and doing that cheap, that is the tricky problem. This is actually kind of in an economy of scale problem. So when we're talking about IoT security, like talking about it as if it was picking right algorithm, um, I think that's talking about the wrong problem. The problem is, how do you write secure software and that's, an economy of scale problem, just like qualities? I mean, how do you build quality into development? I'm going back to, like, code review. So then that means that you can't find a security bugs with one tool or technique, you need to have a whole tool box of stuff. You, need code review, architecture review, you run automatic tests, and you do all sorts of stuff. And basically the way you measure if code is good, is actually by looking up at the suite of stuff the developers have used. So if somebody comes to us and says, I've developed secure code and they can't show any trace of stuff they have done it's hard to trust them.
Researcher: How would be privacy aspect?
AX1: Yes, privacy's is tricky. It is super tricky for a camera company. And it's super important because for us, as a company. I can even say for us as an industry the whole surveillance industry it's really important to not overstep the line because then our whole industry could be regulated out of this planet. Because we are, we are on the border of doing privacy intrusive stuff. Because that's, basically, the whole business model is filming people. So we need to take that really seriously. That said we are in a bit of special uh, so we are building privacy measures into our secure development model, so we're taking privacy into consideration just as we can make decisions on whether some things should be encrypted somewhere in the file we can make decisions on privacy. We shouldn't store this information...
Researcher: Do you automate these privacy decisions or you leave it up to the user consent?
AX1: Yes, oh, so that's the other tricky thing about privacy. So there is a legal aspect where like the contract between the user and the company is one thing in all these legal texts and stuff. We are in a weird position because we're not selling our products to an end consumer. Our products are not being used by the.... but they're actually the privacy breach is not between us and people being filmed. It's between our customers and the people being film. So we're kind of like technology providers we are kind of hidden from a contractual perspective behind that. But from a technical perspective we need to comply to like GDPR and do ah design for privacy, for instance, and that we have built into our processes.
Researcher: I see so the privacy is more the process thing and security is more about technology.
AX1: No, I would actually say that both. So I would say that both privacy and security are process things. That's where I am right now, like on a personal level. I think the technical problems are solvable. But

getting it into processes is what's difficult. And privacy is just one aspect of security. So if I have, like, if I have some sensitive the API key that can leak that has some properties, but if I have, like, social security number that can leak that has other properties. But the tools and techniques for finding them and dealing with them are very, very similar. So privacy by design and security by design are really, really overlapping.
Researcher: Which one is the subset of the other surprise?
AX1: Privacy is a subset of security because it only applies in certain scenarios where there is personal data involved.
Researcher: So there is no privacy without security.
AX1: Yeah, that's basically best it.
Researcher: Yeah, that's good. Anything else that you want to add to this security & privacy of IoT?
AX1: So I want to circle back today where I started out on the whole process thing and Software thing. So I think I think people are putting way too much emphasis on the technical problem, of IoT security. I think that's actually getting it wrong. I think it's kind of putting focus. It's kind of if we just pick the right algorithms and cipher suites, then we can solve the problem.
Researcher: yeah, and they say, like, there is no algorithm which can run on like a small sensor and is secure enough, anybody could break it.
AX1: Yeah, but I'm basically saying that that's the wrong problem? So basically what I am stating now is that if you take most of the companies doing IoT products are not good at doing SW. And because they are not good at doing software or even worse, at doing secure, software. So it means that if you took those guys and gave them the best possible hardware, they would still make an unsecure product. So it's not a technical problem and it's not because they couldn't do the write algorithms because they don't know how to write secure software, and then that is a process problem, it's the awareness and the training of their developers and giving them the tools to write secure software. I think it's very rarely actually come to a point where you need to make a security decision and you're forced to use weak technology because of your hardware platform, I think that's just excuses people have made up.
Researcher: So if you were given a product which is low in RAM and CPU and it has a battery which should run for a year or so, what would be your approach in that case and for security in these kind of products?
AX1: So I would, I think now the tricky thing comes because you're actually giving me a scenario describing the harder platform
Researcher: yeah, like a constraint they are given with
AX1: I'm going to give you a question, which indicates how I'm thinking, and I'm going to ask you, what does the development organization looked like? How many developers are there? But yeah, that's the thing,

if there are lots of developers, then you need to make this a process thing you say I'm not even answering a technical question. So that the only way you could force me to try to solve that problem is, if you would say, it's a constrained Platform it's, a super small team, because then the process doesn't matter. And then I, as an individual, I could go in, and individual contribute to their security by doing code reviews myself, helping them with security sign.
Researcher: So I can clarify my question. So what I'm saying is that it's not possible to implement let's say SHA256 or RSA 4K. Do you think the security is enough in that case?
AX1: Yeah, and that thing then depends on what are you using the thing for. Good that you brought this up, so I'm going to answer it again in my organizational perspective. But I think it works in the other perspective as well. So the way we approach security here is I mean, we have I say, we have, like, a thousand developers, and we're two guys working full time on coaching them, so we can't be all over the place. So what we did was, we made a basically a risk assessment on system level; identifying the most, the high risk components in all the software. Axis is writing, i.e. cloud stuff and camera stuff and pc stuff to us have probably, like, thirty, forty different product deliveries. And then, based on that risk assessment, we started introducing the security work first at those teams. And when we have then analyzed one of those products where we identify threats, we define countermeasures that are appropriate for exactly that threat in exactly that context. So we are very, very context aware in how we define security. So to answer the question for your hypothetical product, you would basically need to say it's doing this in this scenario in this business case because they we can say if it's just doing some silly thing, then it doesn't matter. We can use whatever but if it's actually like a door controller for a bank vault! Yeah, ok, then it's not good enough, but then it could it could be so then it becomes a showstopper. You cannot release that product with that hardware for that type of market.
Researcher: So if I interpret you in my own way, it's like then what you're saying is based on the use case, we do risk analysis and then we come up with security requirements and then put requirements on the platform. This is what we need is, and if you cannot get the platform, then it's not the right time to go out.
AX1: Then it becomes actually like a corporate risk decision.so the hardware is like secondary in all of this. But this is where it kind of tip ties together with like the bill look into your process because if you're trying to ball security on afterwards, you have already chosen hardware you have already made all these mistakes and you already have a schedule on a deadline in and you're going to ship your shitty product but if you build it into the way you're thinking from the beginning. I mean on the first day when a product manager says we're going to make this vault the bank vault opening thingy I mean, even on the first day you're going to buy okay? We can't put any crypto on it .okay? Probably going to pick other hardware. So I think it kind of comes back to that the problems the IoT industry has is because lack of awareness.
Researcher: When you see a lack of awareness, is it in the vendors or it's more on the solution providers?

AX1: I think that's hard to say. I would probably say more vendors because this is a R&D problem.
Researcher: yeah, because these solution providers they completely rely on these vendors and they don't even make a choice. And they just go to buy the cheapest hardware and the platform essentially is not ready for anything and they also have, like based on my study the cost is another factor. So they don't they don't want to have, like, secure chips and security, even like flash area because it's expensive.
AX1: so taking all shortcuts, yeah, but I think we are hoping to do because even I mean our industries also in. It's been a growth market for a long time, but we are now entering the maturity phase where price is going to be more and more important and the way axis or what we were trying to buy, buy ourselves some more time in that in that situation is to actually make security and trust a purchasing factor. So we're going to actively push the way we work with security, and try to charge a premium price for it. I don't know if it's going to work, but it's the plan.
Researcher: When you say trust, are there any more things which are important from enforcing security. Is there something that you it's like a recipe you should always look for these things in your product when you do risk analysis or something?
AX1: Yes, um so I think that's a very, very contextual question it's really hard. I'm not answering any of your questions, I'm answering other questions, but I'll give you a statement related to that. So basically, we consciously chose not to create any security patterns, upfront, okay. So instead, what we did was he started working with the teams and as we work with the teams, we were learning the patterns that work in this organization. So instead of giving them the recipes upfront, we're kind of learning what seems to be like the best practice within Axis.
Researcher: But is it like guidelines. I.e. look for the trust management, look for authorization of things based on the use case.
AX1: Yes, Yes.
Researcher: I can clarify. So basically, I'm like looking for a theoretical model, which I would be proposing in the thesis, and then I'm looking for properties that one should look for when they design or do the system architecture? If you really consider these key things in your thinking process because usually these IoT kind of suppliers, they have no clue about security, and then they just like, they explode the market with their products and it's actually a big risk for Privacy
AX1: Yeah, so I think there are two ways you could try to measure that from the outside the way I like to measure it, is actually by not talking about the product, but instead talking about their process. So I think you should consider that this an alternative, because it's it is starting to happen, it is happening more in other more mature industries. In the bigger software industry it's actually quite common that your customers are asking you about your security development process. They don't care so much about your products anymore, because it's basically too hard to measure. But they can talk to you to figure out, do you

have a security team? Do you do code review? Do you do threat modeling? So that is happening, I think that will happen in the IoT industry as well. It's just behind. So that's one thing, but if you if you really need to look at the product, probably like the stuff that's there for security, like authentication or encryption or whatever that's probably pretty good indicators off how well ah, how good they are! Actually, I don't want use how good they are. I want to use the how bad they are. So probably they have put security stuff in place on places where they think they need to protect something and if they have messed that up with choosing the wrong algorithms to configure it poorly, it's a good indicator that they have tried and have failed, which means that they don't have a competence. But it doesn't necessarily mean that they're even trying to solve the right problem. Because often they put security stuff in place where they don't need it. Because they haven't done the risk analysis. ... Coughing... Sorry for the rant.
Researcher: No, I think I can follow and the risk analysis one way is doing threat modeling
AX1: yeah. For instance. So I mean what you could do as an external reviewer is to look at the product and don't think too much about what security mechanisms they have put in place. Think about the use cases and the business model and start thinking about what you would have liked to see in place and then see if they have done those things. But be aware that security features I wish I had a percentage but to say that security features are like 25% of what's needed to be done to make something secure so if you do like the full security process and try to handle all input validation and buffer overflows the SQL injections and all that sort of stuff . That stuff isn't visible as security features that's just code quality features and that's where the bulk of the issues are. So even if they've done great authentication and stuff yeah you still have the rest and I think that's variety really sucked because again we're not software guys.
Researcher [00:35:32]: So you're thinking or your suggestions are they valid in the autonomous IoT context because most of these devices they are autonomous. They don't depend so much on the human interaction. There could be IoT beneath a bridge and nobody could actually go there and it might still be sending private date
AX1: I think it's super valid because the 'I' in IoT indicates that it's the thing that's on the internet and the guys that are on the other side of the internet looking for weak spots, they don't care if there is a human close to it. They just want the thing, computer or whatever they can attack. And actually, many a times, the attacks don't actually target the thing that was attacked It's, just a collateral damage because you needed a Linux box from which to run your malware that sends spam, to the Taiwanese government. And if that Linux box happened to be an Axis camera we are just collateral damaged. They didn't care about us as a company. And I think that's probably more relevant in the IoT industry as well because you're kind of not really targeting the IoT use case, but you're just grabbing the internet resource.
Researcher: If we change the conversation towards standardization, how does that affects the SW development process and decisions that we make from a security perspective? And so does it matter to have

standardization or it's fine, everybody use their own.
AX1: So I think that standardization is good because we shouldn't have too much options, whenever we have freedom to choose, we have the opportunity to choose poorly. So standards are good in general because then basically anybody can make something that's decent because they don't have to make that much of a choice. That is especially true in, like from a technology perspective, because all the standardization is really technology focused. When it comes to this process integration and work flow one there is very little standard says shit done. There are some attempts, there's, some stuff done, but it's not at all as mature. So in that space, I think standardization is not relevant yet. Things aren't mature enough.
Researcher: So are you pointing towards these ISO for security requirement.
AX1: Yeah, ok.
Researcher: And they're not enough or so.
AX1: Yeah. There are like two schools. Like ISO27000 etc... Many of these come from an IT environment.
Researcher: Exactly
AX1: And actually I think they are bad for security. Because what happens is that you create policies based on some theoretical model that forced you to do something would have thinking about your context she's actually spent a lot of time implementing stuff for no obvious reason instead of starting your brain and doing. So, I think they're dangerous. But there are open SAM and BSIM and other models on how to right secure software. But they're not prescriptive they're more descriptive and giving examples of what people are doing like you could do threat modeling, but that's where the research is lacking because you don't really know nobody really knows how effective is threat modeling ? How effective is code review with some certain tools so we're using a lot of stuff, but you don't know how good it is and that's why I'm why I am saying that standardization isn't a good thing yet because we don't know what works yet from process perspective. It is little bit like the black magic still.
Researcher: we have lots of standard from the product point of view like the software standards and communication technology it's like multiple standards. So I don't know what your view on that is. They have to use some standard e.g. BT standard or ZigBee, WIFI, but then there are so many of those and how do we cope with that in IoT.
AX1: That's a tricky thing. Again, it makes things more difficult if you have to choose to technology and then once you have chosen technology, you actually needs to choose implementation and that's a third party implementation. I mean there's a lot of choices where and even when you picked something you still need to configure it correctly so there you have a lot of opportunities to make mistakes. So simplification would be good. But it's basically puts us back to the same old problem as writing any software which is still the point I'm repeating. So if we think about IoT stuff as SW development yeah it's just like any other software

development project where you have a lot of choices to make.
Researcher: So look for the use cases, do the risk analysis and then have a good process and awareness among the developers, that's basically the recipe.
AX1: Yes, that's basically the general recipe which can of course fail utterly because it's a super... it's a personal thing and it's not a technical thing anymore and that's much more difficult.
Researcher: I see. Any last statement that you want to make to the IoT community, something that you want the IoT guys to think about or do.
AX1: I think it is related to learning from other more mature software industries. I think that's what they should do. They should not try to invent all this stuff because they're not the special snowflake. I mean, I don't want them thinking about themselves as a special industry. They are just software developers, like any other software developer, and they should learn from the others. They just happened to be the new kids in town. I mean, they're basically the new kids connected to the internet. There have been other industries connected to the internet before, and they have coped and learned from that.
Researcher: So the key here is like how to get protected from the public network.
AX1: Yeah and they are no different from any other thing that has been developed in connected to the internet since it was formed in the seventies whatever it was.
Researcher: I think it's a very good concluding statement. Great thanks a lot. Really appreciated.
AX1: thanks. Nice seeing you again.
Researcher: Thanks.

Appendix F: Interview of HX1

HS1: Security has become very much a band aid business when you find a new hole let's put some plaster on it and if you find a new leak there is someone with a concrete slab. The problem is that this is happening faster and faster and faster, security hole and security. So what did they do? Well they invent even more intelligent but reactive tools like AI. Because people are fast enough to patch so we will have robots that patch instead of rethinking and doing it right which we had done. So we have a completely new architecture for security. We are decentralized focused and not centralized focused. So it is secure technology but comes from messaging thinking but if we have adapted it so it fits perfectly to any IoT system especially distributed applications like IoT.
Researcher: Can you give me a little bit more background? Little bit more about your business and how you relate yourself to IoT?
HS1: I started many years ago in customer project management. I worked in IoT industry, I worked in Telecom, I worked for Ericsson, and I worked for lot of these companies. Handset is a Terminal to the internet. It's not the machine, it is a human interface, human internet interface this is Terminal and that's where it's heading now. So when I was a developing app project like five years ago where we wanted to position people have a positioning on request I wanted position of your phone without the involvement of operator or governments and it has to be responsive so you shouldn't be allowed to track, i.e. there would be no tracking because the positioning today still works with tracking. I take a position on my phone and store it in database the problem is that all that information is unnecessary usually because I'm not interested in the way of being, I am interested in where are you right now when I send the query that's what I want to know. So all that sending just extracts unnecessary energy from the battery, it takes a lot of unnecessary data traffic and we tailored this application to find people in the mountains. I also wanted to find kids, I wanted to keep track of my kids. That was the use case. So we had discussions with Chinese manufacture, one Android based GPS positioning tag which was a very early IoT device. We developed a cloud based message broker system for position queries. That was kind of a complex thing to do. Since we have developed a message broker technology that was privacy protected because we don't want to have a stalker's tracking my kids. So we have thought about those things. No trail of information, we always cleared logs and so it was ephemeral messaging like snapchat. Real ephemeral messaging is some message it's consumed and then destroy and vanishes for good? We have done that but for positioning ephemeral positioning, responsive position. So we realized that if we put a security and encryption layer on this then we would have the world's most secure communication system. Then we thought that's probably some money in that. So we implemented PGP architecture based security layer on that you could do messaging because PGP is for some sort of message. Asynchronous communication. We have that and we started selling this enterprises and developers.

HS1: I take your public key. I encrypt with your public key then it can only be decrypted with your private key this means that I have to know who I encrypt for. That's how it works. That makes it extremely impractical for IoT and for MQTT protocol because you broadcast and you consume and broadcasting device does not have a clue who is consuming. It doesn't work for IT system because if I put something in a database and it will be consumed two years later, how should I know. So what we did in the custom project is that we turn this around so we were in fact do is encrypt for no one but encrypt specific key, each data maps with symmetrical key and I as the device or the end point still owns the key. Retroactively, at consumption stage, the consumer ask me for the key and then we send the key. The symmetrical key will be sent in an asymmetrical way. What it does is that it turn everything around. If everything can be locked down all the time and can be decrypted at consumption stage you can store that data in China if you like. You can send it on any technology, you can do whatever you like. And suddenly MQTT works into encrypted. So that's the new Architecture. "We can do end-to-end encryption for anything in any communication patterns and any storage". We have a security layer that works for any supplier. If you large system, you probably have amazon cloud and Azure cloud or Unix cloud and you have mix of those things and then you have one security model there and one there and one there and it gets extremely complex and you know what happens with complex systems, there will be billions of security holes. So we just add security layer on top of that. We lock down the data. We can do that in from cortex M3 and upwards. We usually need Linux. We have SDK (in C and Java) that you implement as an app developer. We have a variety of all the wrappers around those things.
Researcher: I am just curious about the asymmetric part of the protocol. So how do you exchange keys when the end point is requesting to get symmetric key.
HS1: Using signal like protocol used in Snapchat and WhatsApp. So then it is an overhead for the system that you have to do these extra transactions.
Researcher: But how do you establish the trust?
HS1: I cannot answer that but we have it in our whitepapers. In IoT the problem is that the end point is dump ad goes to sleep all the time in order to save battery. We have delegation technology so you can either delegate a key to a group manager still very distributed but it might be a centralized in sort of group of sensor, usually gateway that actually has power and is alive all the time because it manages the traffic. It would also then manage and have storage off encryption keys. If that's not enough you actually still need back up of that private key we can make a local backup but in the cloud with no access from cloud which is us. We cannot access the key because we use Intel SGX (Secure enclave) to store pre-generated keys and backup keys. In order to extract you need to have a strong authentication. We also sell an application which end-to-end encrypted drop box for government and for lawyers or anyone that has a problem with GDPR. Extremely easy, simple solution, but where you might need to change devices that you might need

to be able to the recover everything and recover the key. We then connect it to mobile bank ID or 2/3/4 factor authentication.
Hyker is two things: we are a encryption key broker as a service and the technology is today licensed will be become typically as SONY does it i.e. dual licensing scheme within open-source part and when you go commercial license part if you want the whole technology. **Instead of just adding AI and other stuff and look how people behave and this is and that, we instead lock down all the data**. The fundamental thing, we don't need a network security we don't need anything, we just need to protect the end point and the data. We don't protected the end point we just protect the data. When it's generated to when it's consumed it is completely locked down. We use AES 256 etc. All the encryption is standard. Everything is standard. It's prepackaged and easy to use for developers with the twist of the extra key distribution. If you brute force one key only one data set is lost. We have billion keys for system. It's a tradeoff, you lost one data or you go to stronger security, AES-512 etc. All those algorithms are open-source so we just take one.
Researcher: I think it was really interesting to listen to you I will try to connect it with my research.
Researcher: A couple of phrases you mentioned or highlights, one was end to end security you mentioned multiple times so can you elaborate on how important it is in IoT and second thing I heard is like instead of looking at the overall holistic view we should narrow down the problem to the root cause or the most important thing what needs to be protected.
HS1: And those two are actually combined because the thing is that data is flowing everywhere and IoT will be even more. All data is out in the public there are two things that will be confidential data flowing in the public that has to be protected but also there will be a lot of data which is not for free so it's not confidential per say but it's actually something that someone want it to charge for. If you go into a small city, it would have a lot of applications in it and they will be somehow integrated, there will be analytics on, there will be a lot of data providers, most of them commercial, they will not give away their data to the city. Usually the power company, the water company will not give this away, the house company will not give away the data. Will Mercedes give their data to Volvo for the traffic management system? Probably not. Everyone wants to get return of investment, so everyone wants to charge for this. IoT Sweden has come to this realization in the academic world, but not in the business world yet that the data has to be locked down, open up in real time and traded, must be able to trade it and charge for it per data element. There will be a spot markets, there will be data stock extensions, where people buy and sell data. To be able to do that you have to be able to lock it down. I as a data owner I want to maintain control of my data, even though it's stored in your database. So how did you develop that is fundamental for data flow in IoT? You will have multitude of data owners in the same application, we will have multitude of applications all this in a big mash up.
Researcher: Do you think blockchains is some kind of solution.

HS1: No. No. blockchain is integrity and accessibility based upon the notion that everything should be public. You can't use that for confidential data unless if you use Hyker security layer because we are 100% blockchain compatible. We provide the confidentiality, then you could have the data flows and data stores and integrity and all those things. Because in that block we would just say this is the data owner, ask him for the key and this is the data that is encrypted. This is the address to who asked for. Then you will have a request for the key and the device would say yes or no depending on business logic a part of the delegation system we have. You could develop a system that always have managers that you ask, am I allowed to? They will not have override to say you must but if they will always have possibilities a vito to say no. Because that's what security is about saying no.
Researcher: How can all this be automated if you have this big boss kind of manager who is authorizing certain nodes or things who could access?
HS1: That's part of our protocol. So you just set up white list and black list. That's what we handle. It might be part of the blockchain.
Researcher: Is blockchain practical for IoT system with very constrained resources?
HS1: Depending on what block, I will say not really a blockchain but IOTA type which is not based on blockchain but has a similar effect. Because then you don't have any problems of mining. They have pre-generated all the keys. Distributed ledger kind of technologies will be fundamental for this. But we are in very early generations.
Researcher: But all these computations will happen somewhere in cloud or other intermediate gateway.
HS1: Personally, I think you should push computing power as far out to the edge as possible distributed because these enormous amounts of data you can't have a brain processing it. It should come pre-processed all the way through the change meaning that the first processing will be in more intelligent hub or a gateway to the stupidest sensors and that gateways is our endpoint in our world. Because that's where we do the encryption and that will also keep its own private key in the gateway.
Researcher: Academics usually talk about constrained resources in IoT and things, so is it not a problem?
HS1: It is problem but you have to take in a practical approach. How far out can you maintain processing power? How far can you maintain power?
Researcher: But if you don't have to reach the end point or the sensor itself, then it's not a real problem as such, right? We already have the solution, we already have the architecture which can address those problems.
HS1: We call it fog computing, we call it edge computing but what it means is that I mean you put a lot of processing power in the end point or as close to the endpoint as possible. Those are group owners of the stupid devices. That is how I perceive from a practical point of view because then you can have a sense that goes asleep where battery lasts for the lifetime of the device. No customer is really mature enough to start

it. **Security in IoT is a joke**. Because the customer's implementations hasn't really gone live yet. Security is always retroactive, it's something that happens when people say oh shit. You can forget about AI and you can forget about all stupid things. You will need that processing power for many things like analyzing data and doing good things with the data not for preventing people from using the data.
Researcher: You mentioned like IoT so many times. So what exactly is this internet of things for you?
HS1: Nothing. It's just stupid buzzword. For me, it's all about applications. In my final application that for me I have a Google home. I turn on the light, I have all these things, they are just application. Voice control of my light. Another application is autonomous car. Traffic management, Queue management. It's all about applications. IoT for me is just a stupid buzzword because it actually takes the focus away from the application. The application always has a case it solves a problem, IoT doesn't solve anything, it is just like a cloud. Another person's computer that leases to me okay that's what cloud is. Then there are a lot of fancy architecture to make it more and more agnostic. Like Dockers, containers, etc., the heart of the system, and those are the actual tools that develops the applications. IoT is just a fancy word.
Researcher: Is there any essential elements in IoT that defines it as IoT?
HS1: No. I don't see that even though that IoT itself is more problematic than other IT
Researcher: You used the word IoT so what exactly is this IoT?
HS1: It's a buzzword that you connect everything. Everything connected for applications. Internet is TCP/IP. So you can have IoT without internet but you need to have connectivity. IoT for me is about connected things to other things.
Researcher: So IoT is really not about internet of things but it's more about connectivity of things.
HS1: Connectivity of things and distributed intelligence. Maybe it's just a network segmentation you're talking about. It's good that user owns various technology because it prevents a lot of things but you shouldn't fool yourself in thinking that it's protection enough. What is protecting that computing power or computing environment somehow? Biggest problem with IoT is that with the word IoT, I can connect anything. Industry 4.0, I can connect anything to SCADA system, I connect anything or I can take that printing machine and connect it to IoT so I can measure things and having dashboard in the iPad, great stuff, OT systems have never been built for end security because they've always been offline meaning that we are about to kill the whole western world industry. Internet of things merges a lot of different industries with their standards or lack of standards. There are more than 600 different protocols in IoT so how do you develop security for this. One approach says everything has to be TCP/IP, then that's not utilizing the strength of technology. Everything has to smart, everything has to have 5G this is not an IoT. IoT has to be very small probably a sensor, a stupid sensor. **You need a unified security model to protect it**.
Researcher: What is your view on openness, open-source.
HS1: Open-source like any process has its benefits and drawbacks. Open-source in maintained active

community that's the most powerful thing. An open-source that is controlled by one player and half asleep that's lethal the system because it will have security holes bugs that will not be fixed in time. So in some cases it is better to have an active body or corporation, old government, maintaining their code and doing it part of their business. So open source is not a solution to everything, but is solution to invention, to innovation, to all these things. Open-source is fundamental to IoT. Its fundamental security because you have to be able to do and test the code, and see the code. That's why we do all the encryption based on the open-source libraries. Because they approved by market and developers, e.g. openssl. But some parts are not open source today because we need to have controlled owner and that's the key distribution part so that it's our own proprietary solution. If we will, when this matures, we will release a lot more in open source or in fact the dual source. (Open-source but if you go commercial, you have to pay license).
Researcher: When we talk about open systems or open-source do they consider security as one of the important thing?
HS1: No. It is usually considered maintainability and innovation.
Researcher: In research terms like flexibility, customizability and extensively are used but do you think security is missing.
HS1: Absolutely. Because security is boring is a generic perception. Because security approach is often about prevention you're not allowed to. But with Hyker approach yes you can do all these things but you have control. Security is not about locking in it is about freeing data. Notion that I use is **secure open data.** Open data will only be open as long as you can protect the commerciality of data.
Researcher: What does security means to you?
HS1: From business point of view if I generate data, I want to secure it. It is about protecting my assets. I want to get paid for that. It's exactly like if you're a rock star and you released a new song on Spotify and you want to get paid for that. So I think for me, security will be very much about digital rights management conceptual wise. Some data will have very strong digital rights controls like government or your private data in accordance with GDPR. In accordance with the GDPR law, you should actually have full control of all your data i.e. you should own the rights to all the keys to your data. So in essence our technology is the first and only implementation of GDPR in IT.
Researcher: Is GDPR about privacy or security?
HS1: For me, GDPR is about respect. This is you and that is your data is your digital twin of you. I respect you as a person. You're allowed to live so it's your data. It's about democracy, it's about respect for the individual and it's about being human, respect for humanity. It's forcing you to respect the individual you to business with.
Researcher: Is that more about privacy?
HS1. Privacy is just another term for confidentiality and ownership. Because you have a lot of data that you

own and that you might want to have confidential like your bank account or something else. For some people it's very important to hide how their sexual appetite for other people it is extremely important to hide their ancestry because of situation. If you respect people they should be allowed to have secret.
Researcher: They do share their data with certain people or organization and then they trust. Is it more about trust management? They are not really keeping it confidential.
HS1: Yes, it is. It's about respect that you have released this data into the public domain. You have released that data but if I do lot of analytics and tracking on you, I'm actually gathering data that you have not released to the public domain willingly. **A person is no different from the IoT device it's just an end point**. Today you have a hub for all your cybernetics that you have installed and some are not connected. You have a lot of cyber tech already in you or on you. You also have probably AI. All those thing are already there, the thing that's happening right now is that those things are getting connected that actually provide new applications. It might be that we actually distribute that gateway, that terminal intelligence even more into the end points which will be then incorporated. Humans are just another end points. IoT is about connecting machine to machine, but it's also about connecting machine to machine to humans and doing applications on that.
Researcher: Do you think the existing mechanisms and tools to handle security or privacy in IoT is sufficient? What is that makes it in sufficient?
HS1: No. Complexity. Complexity and the multitude of standards. If you have too many standards in an application it will be un-manageable. Just take a very simple system, take a zee wave smart home and connect it to the internet, where is the security in that? Well they have one encryption technology in the latest version of zee wave. You might have TLS to cloud service somewhere and there is in clear text if the cloud provider encrypts it in a database. They still have the key, you still have to trust them. So where's the security? It's about I had to trust amazon and their personal and processes and their sub suppliers processes and the bleeding hard drive manufacturer in Korea. I have to trust them. We see that it's not always possible. **You have to do a cost benefit analysis to see what's the value of my data** and what kind of risk budget can I have on my data. I in my organization or as a person. But people aren't educated and have understanding, you have to build applications to do this for people. Easiest thing is to lock everything down and you provide openness only when allowed. Today all data is open in some stage, in the transportation, when you handout between TLS and into the database, an insider or malware or hacker or whoever, government, cloud act, any Trump agent, Any American company, they will have more data. Period. They can promise you in their marketing leaflets that we have encrypted database and we use this and that but they still have the key. People still use Dropbox because they think that the value for my day is so low that I could give it away for free to anyone.
Researcher: So what you're emphasizing is point to point encryption?

HS1: Hop by Hop and Point to Point both. How do you make management system that actually manages to control all that data in all these street technology environments? It has to be fully automated because you cannot have people doing this. You cannot even have people doing manual set up for this it has to be automated, installation must be automated, handshake must be automated, and everything must be automated. Because it's too complex, it's too complicated and it happens too fast and we can't have latencies and there are millions of devices pouring out right now every day. You cannot manage that, it has to be self-managing. That's one of reasons why everyone talks about blockchain because if it guarantees manages trust but it does no protect confidentiality.
Researcher: Is security for you tools and mechanisms or is it more about the process and people?
HS1: Yes, for me it's about developing the right tools. **"The only security worth anything is the one that's being used or the only security worth anything is the one that you never even notice**". So people accepted computers when they stop being computers became a TV set or handset or something. People will accept security or use security if it somehow hidden. I think that is the most important thing. When that works, you can actually start working with what people do I trust in organizations. Should I trust this guy that's, newly employed? How much data should he have access to? That's people management and then we develop processes. But without technology solutions, people will always take short cuts. If you heard about the term shadow IT, shadow IT it's about 50-60% of all the global IT budget. And what is that? It is a drop box and email, because the things that's being provided by the ones responsible in IT and security, it doesn't work in my job. My job is fulfilling these tasks then I get paid but it never says, and do it securely. How do you measure that? You don't. So you have to start with a system that is fundamentally secure.
Researcher: So do you actually create security? Is it by having the right process in place and how you develop the code? Or it's more about which algorithms will be used?
HS1: Start with architecture. Seeing that there are no possible or theoretical holes in this.
Researcher: Should we do like risk analysis and threat modeling.
HS1. I think start with that. This is a whole complex system, these are all the access points, and these are all the users these are all the producers and consumers. This is the data it's storing. We don't want to have this in the bank vault, we want to have it in amazon, ok Amazon is a risk, let's eliminate that risk. Instead of trying to find we cannot do this and this protocol because there are holes, eliminate the whole problem.
Researcher: Should we think about security from beginning?
HS1: Secure is part of the architecture system so if you have a system architect that does not implement security completely then he should be out of a job. **Its fundamental, fundamental things that always should be part of the architecture. Its latency, its back up and its security and it's all these things it's just things that have to work**.

Researcher: How about the software upgrades in open IoT system or open secure IoT system? How important is software upgrade and what's the relation between software upgrade and security?
HS1: Security today you do a fundamental architecture but there will still be mistakes and things will change because it's so complex. I had meeting with physical security people not IT security yesterday over lunch. We talked about security, secure systems and I asked them, we have this secure application for document management. How often do you see we do new product release? They said oh it's going so fast now a days so maybe you do that every six mont**h** or every month. No every Friday. And that's slow. Because things change all the time. Building software, building applications, you build upon so many components that are in constant development. When you do this kind of application the web browsers changes, new releases all time. And the fundamental HTML standards changes. Then you go through the stack everything is in constant development meaning there will be new things that worked today will not work tomorrow and day after tomorrow is a huge security hole. You can see that from processor architecture, etc. **The only thing that you can do from security point of view is patch**. IoT device that cannot be remotely patched automatically without manual interference will never enter my room. Period. So **SW updates is essential in how we develop. It is a continuous process** you patch all the time.
Researcher: And this understanding is missing in IoT user?
HS1: A lot of things are missing. I have had interesting discussions with LoRa (low bandwidth, extremely efficient in battery) people about how you do remote updates on why and how. Laura itself works if you do a side channel. Have LoRa for the communication and then you can send notification you have an update mate and then it wakes up 5G or whatever. It will not be cheap device, but you have to do this. You have to be able to send a chunk of data. So it must be more intelligent than we have today. If you're not just a stupid temperature sensor because when it dies the only ways is to put a new one. As soon as it generates important information then it should not be generated by one of those cheapest, stupidest devices. It should be more intelligent, being able to patch it, being able to control it, control the integrity of the data.
Researcher: I think this was a very valuable statement that we should design the hardware based on how critical data is.
Researcher: Do you want to make any last statement for IoT community and developers. What you want them to tell or do.
HS1: I want them to think about end to end security, really. It's about harnessing the value of the data that product generates because the one that buys that data will do it for a purpose. That data will have a value to it and that customer won't protect this value. You should think about the whole process. You are not developing a temperature sensor you're developing a component that's being used for some purpose. So you have to think about end to end.
Researcher: Thank you so much. It was pleasure to interview you.