



**Identification of security threats to data privacy
posed by smart appliances in home area networks**

KT Nshimba

 **orcid.org 0000-0002-0709-1123**

Dissertation accepted in fulfilment of the requirements for the
degree *Masters of Science in Computer Science* at the North-
West University

Supervisor: Prof R Goede

Co-supervisor: Dr C van der Vyver

Graduation: May 2020

ABSTRACT

The adoption of smart technology has seen great increase in the past few years, at the core of this increase is the affordability of hardware such as sensors, microcontrollers, memory, and open-source operating systems that are based on the Linux kernel. By putting this hardware into an ordinary appliance such as fridge, coupled with an operating system, you have a smart appliance. A traditional home area network that once comprised only of computers and other Wi-Fi gadgets now has smart objects connected to it and the result is a smart home. The interconnection of IoT devices in a smart home, no doubt, brings many benefits to homeowners, but it also introduces privacy concerns.

The design of smart devices depicts a four-layer architectural design. The majority of the devices have sensors to gather data from their surroundings (perception layer); the devices have network capability using different protocols (network layer); certain devices have the ability to store data on the internet as cloud storage (support layer); and most devices are equipped with, or able to connect with, a user interface (application layer). This four-layer architecture is used in this study as a theoretical framework to understand and identify concerns regarding Internet of Things components.

After a theoretical investigation into Internet of Things components and computer security aimed at understanding the security concerns of these devices, the results of an interpretive empirical investigation are presented. The aim of the empirical investigation is to understand the security concerns of specific devices and appliances based on the manufacturer's selection of specific hardware and software components. From the analysis of the data it is evident that policies on gathering, transmitting, storage and especially sharing private data are posing the greatest risk to home owners.

The research also discusses ways of mitigating security issues that may exist due to the addition of smart devices into one's home. This is achieved by creating guidelines that can help each homeowner to be more knowledgeable about the type of smart device they plan to add to their network, by identifying the security concerns and providing a way to mitigate these concerns.

This study is structured as follows: Chapter one introduces the research by highlighting its objectives; in Chapter 2 the research path this study is taking is identified; in Chapters 3 and 4, background information on Internet of Things and computer security are given; in Chapter 5 a comprehensive empirical investigation on the collected data is carried out; in Chapter 6 findings of the research are discussed; and in Chapter 7 a conclusion of the study is given.

Keywords: *Home Area Network, Smart Home, Internet of Things, Security, Privacy, Cyberattacks*

ACKNOWLEDGEMENTS

I would like to say thank you to my supervisor, Prof Roelien Goede, for not giving up on me through the many years of this study. Without her mentoring, encouragement, and patience, I was never going to reach this milestone. I thank your family too for allowing you to take time away from them to help me.

I would like also to thank my co-supervisor, Dr C van der Vyver, for his contribution, especially with the literature review chapters.

Since English is my third language and most of my early education was in French, I appreciate the efforts of the critical language reader Elmarie Engels to reduce the language errors in the document.

To my wife Ruth Makhosazana, thanks dearest for your support and understanding. You have been my support system for many years, despite all we have been through you still believed that I could finish this and never to give up. I love you for allowing me to take time away from you to work on my research.

To my two daughters Kaja and Clarisse, you probably never understood what daddy was always doing on the computer writing and not playing with you. One day I will explain to you what I was doing. Thank you for not disturbing me and for giving me space to concentrate, daddy loves you.

TABLE OF CONTENTS

ABSTRACT	I
ACKNOWLEDGEMENTS	III
TABLE OF CONTENTS	IV
TABLE OF FIGURES	X
LIST OF TABLES	XI
CHAPTER 1 INTRODUCTION	1
1.1 INTRODUCTION	1
1.2 CONCEPTS KEY TO THE STUDY	2
1.2.1 Internet of Things	2
1.2.2 Network Security	3
1.2.3 Data Privacy	3
1.3 PROBLEM STATEMENT	4
1.4 OBJECTIVES OF THE STUDY	4
1.4.1 Theoretical sub-objectives	4
1.4.2 Empirical sub-objectives	5
1.5 RESEARCH DESIGN AND METHODOLOGY	5
1.5.1 Research paradigm	5
1.5.2 Principles of interpretive research	6
1.5.3 Research Methods	7
1.5.4 Rigour and evaluation of methods	8

1.5.5	Delimitations to the study	8
1.6	Ethical considerations	8
1.7	Chapter classification	9
1.8	CHAPTER SUMMARY	10
	CHAPTER 2 RESEARCH METHODOLOGY	11
2.1	Introduction	11
2.2	Research paradigms	12
2.2.1	Positivism	13
2.2.2	Interpretivism	13
2.2.3	Critical social theory	14
2.2.4	Design Science Research	15
2.2.5	Position of this study	16
2.3	Interpretive research methodology	16
2.3.1	The fundamental principle of hermeneutics	16
2.3.2	The principle of contextualization	17
2.3.3	The principle of interaction between the researcher and the subjects	17
2.3.4	The principle of abstraction and generalization	17
2.3.5	The principle of dialogical reasoning	18
2.3.6	The principle of multiple interpretations	18
2.3.7	The principle of suspicion	18
2.4	Interpretive research designs	18
2.4.1	Case study	19
2.4.2	Action research	19
2.4.3	Ethnographic research	20
2.4.4	Archival research	21
2.5	Qualitative versus quantitative research	22
2.6	Qualitative data collection	23

2.7 Qualitative data analysis methods	23
2.7.1 Grounded theory	24
2.7.2 Content analysis	27
2.7.3 Interviews	31
2.7.4 Grounded Theory	32
2.7.5 Document research	33
2.7.6 Position of study	34
2.8 Detailed research plan of the study	34
2.9 Summary	35
 CHAPTER 3 INTERNET OF THINGS	 37
3.1 Introduction	37
3.2 Smart appliances and devices	39
3.2.1 Selection of smart appliances and devices investigated in this study	39
3.2.2 Benefits of smart appliances in a household	46
3.3 Smart electricity management	47
3.3.1 Smart electricity grid	47
3.3.2 Smart meters	47
3.4 Sensors and sensor nodes	49
3.4.1 <i>General-purpose PCs</i>	49
3.4.2 <i>Dedicated sensor nodes:</i>	50
3.4.3 <i>SoC nodes</i>	50
3.4.4 Design characteristics of the sensor node	51
3.4.5 Radio Frequency Identification	52
3.4.6 Actuators	53
3.4.7 An example: Nest thermostat	54
3.5 IoT Gateway	54
3.5.1 Security concerns of IoT gateways	56
3.6 Operating systems of IoT devices	56
3.6.1 IoT based operating systems	58

3.6.2	Security issues in IoT operating systems and applications	61
3.7	Networks	62
3.7.1	Historical development of the internet	63
3.7.2	Categorisation of networks	65
3.7.3	Local Area Network	67
3.7.4	Wireless Networks	69
3.7.5	Security in wireless networks	75
3.8	Security implications for smart homes	79
3.9	Summary	81
	CHAPTER 4 SECURITY IN A HOME AREA NETWORK	83
4.1	Introduction	83
4.2	IoT in context of traditional computer security	84
4.2.1	IoT in context of hardware security	85
4.2.2	IoT in context of software security	86
4.2.3	IoT in context of data security	87
4.2.4	IoT in context of network security	88
4.3	Security Vulnerabilities, Threats, and Attacks	91
4.3.1	IoT security vulnerabilities	92
4.3.2	IoT network security Threats	94
4.3.3	IoT security attacks	95
4.4	Data protection: Cryptography	99
4.4.1	Classical cyphers	100
4.4.2	Modern cryptography	105
4.4.3	Cryptography and network protocols	111
4.4.4	Current cryptographic solutions in IoT and their limitations	112
4.5	Summary of IoT security to consider in empirical investigation	113
4.6	Summary	116

CHAPTER 5 EMPIRICAL INVESTIGATION	118
5.1 Introduction	118
5.2 Data collection and analysis strategy	120
5.2.1 Data collection strategy	120
5.2.2 Data presentation and coding strategy	122
5.2.3 Strategy for the formulation of findings	126
5.3 Smart televisions	126
5.3.1 Data collection for smart TVs	126
5.3.2 Data presentation and coding	127
5.3.3 Smart TVs findings	138
5.4 Smart Speakers	140
5.4.1 Data collection for smart speakers	140
5.4.2 Data presentation and coding	140
5.4.3 Smart Speaker findings	151
5.5 Smart Locks	152
5.5.1 Data collection for smart locks	152
Sense™ Smart Deadbolt Z-Wave plus	153
5.5.2 Data representation and coding	153
5.5.3 Smart Locks Findings	160
5.6 Smart Fridges	161
5.6.1 Data collection for smart fridge	162
5.6.2 Data presentation and coding	162
5.6.3 Smart Fridges Findings	170
5.7 SMART GATEWAYS	172
5.7.1 Data collection for smart gateways	172
5.7.2 Data presentation and coding	174
5.7.3 Smart Hubs Findings	185
5.8 Summary	187

CHAPTER 6 GUIDELINE DEVELOPMENT	189
6.1 Introduction	189
6.2 Generic guidelines from IoT architecture	191
6.3 Security concerns of smart TVs	196
6.4 Security concerns for Smart Speakers	198
6.5 Security concerns for Smart Locks	199
6.6 Security concerns for Smart fridges	201
6.7 Security concerns for Smart gateways	203
6.8 Summary	205
CHAPTER 7 CONCLUSION	206
7.1 Introduction	206
7.2 REFLECTION ON THE OBJECTIVES OF THE STUDY	206
7.2.1 Reflection on theoretical objectives	207
7.2.2 Reflection on empirical objectives	213
7.3 contribution: Guidelines for home owners	216
7.4 Evaluation of research	219
7.4.1 Principles for interpretive case work	219
7.4.2 Limitations of the study	221
7.5 Future work	222
7.6 SUMMARY	222
BIBLIOGRAPHY	224

TABLE OF FIGURES

Figure 2-1 Action research spiral adapted from Saunders (2011:148)	20
Figure 2-2 Cycle of data collection and analysis in grounded theory adapted from Urquhart et al. (2010:363)	25
Figure 2-3 Content analysis steps (Elo & Kyngäs, 2008:110)	29
Figure 2-4 Induction, deduction, and verification in grounded theory (Heath & Cowley, 2004:144)	33
Figure 2-5 Research decision-making structure	34
Figure 3-1 A representation of a smart home (Smarthomeenergy.co.uk, 2019)	37
Figure 3-2 Comparison of a traditional electricity meter and a smart meter architecture (Depuru et al., 2011:2737).....	48
Figure 3-3 Components of an RFID system (Jia et al., 2012:1283).....	53
Figure 3-4 Structure of a computer-communication network (Kleinrock, 1976:1327).	63
Figure 3-5 ZigBee protocol stack (Anon, 2011; Ramya et al., 2011:299)	73
Figure 3-6 ZigBee logic topology (Varchola & Drutarovský, 2007)	73
Figure 3-7 Overview of security threats in a ZigBee network (Karnain & Zakaria, 2015:2)	78
Figure 4-1 Aspects of computer security, adapted from (Carroll, 2014:8).....	85
Figure 4-2 IoT architecture, adapted from (Ali et al., 2019).....	92
Figure 4-3 Caesar cypher (Luciano & Prichett, 1987:2)	101
Figure 4-4 Caser cypher in decimal representation (Luciano & Prichett, 1987:2).....	101
Figure 4-5 An example of columnar transposition	105
Figure 4-6 Basic operation of a symmetric key cryptography quoted from Anjum & Mouchtaris (2007:20).	106
Figure 4-7 Asymmetric key cryptography quoted from (Stewart et al., 2012:406)	107
Figure 6-1 IoT architecture, adapted from (Ali et al., 2019).....	191
Figure 7-1 IoT architecture, adapted from (Ali et al., 2019).....	209

LIST OF TABLES

Table 3-1 Comparison of smart locks adapted from Delaney (2019)	42
Table 3-2 Comparison of smart cameras features, adapted from Wollerton (2019)	45
Table 3-3 List of researches conducted on smart grid technology and its security.....	48
Table 3-4 List of common sensors and transducers (ElectronicsTutorials, 2015)	50
Table 3-5 Comparison of Current IoT Operating Systems (RIOT, 2015).....	60
Table 3-6 Characteristics of wired and wireless networks (Navpreet & Sangeeta, 2014).	66
Table 3-7 List of wireless protocols (Postscapes.com, 2019)	70
Table 3-8 Categories of IEEE 802.11 standards (Pi Huang, 2016).....	71
Table 3-9 Intuitive identification of vulnerabilities based on IoT network architecture	80
Table 4-1 Network information gathering tools (Hoque et al., 2014:310)	90
Table 4-2 Network scanning tools adapted from Hoque et al. (2014).....	91
Table 4-3 Vigenère square (Kester, 2013:142).....	103
Table 4-4 Number of transformation round (No) vs. Block length (Bhaskar, 2008:85)	109
Table 4-5 AES encryption and decryption algorithms (Lu & Tseng, 2002:2)	109
Table 4-6 Updated security aspect based on IoT network architecture	113
Table 5-1 Example of manufacturer data source.....	121
Table 5-2 Example of coding of manufacturers' documents.....	124
Table 5-3 Coding example of online reviews.....	125
Table 5-4 Smart TVs data source.....	127
Table 5-5 Representation of manufacturer's documentations	128
Table 5-6 Data from Reviewers on smart TVs	133
Table 5-7 Smart speakers data source.....	141
Table 5-8 Representation of manufacturers' documentations	142
Table 5-9 Representation of reviewers' documents.....	146
Table 5-10 Smart locks data source.....	152
Table 5-11 Representation of manufacturer's documentations	153
Table 5-12 Representation of reviewer's documentations.....	156
Table 5-13 Smart fridges data source.....	162
Table 5-14 Representation of manufacturers documents	163
Table 5-15 Representation of reviewer's documentations.....	166
Table 5-16 Smart gateways data sources	173

Table 5-17 Representation of manufacturers' documentations	174
Table 5-18 Representation of reviewers' documentations.....	179
Table 6-1 Security concerns of IoT networks from a theoretical perspective	192
Table 6-2 General Guidelines for all IoT devices.....	194
Table 6-3 Security concerns from data analysis for smart TVs.....	196
Table 6-4 Additionall smart TV guidelines.....	197
Table 6-5 Security concerns from data analysis for smart speakers	198
Table 6-6 Specific smart speaker guidelines.....	199
Table 6-7 Security concerns from data analysis for smart locks	199
Table 6-8 Specific smart lock guidelines.....	200
Table 6-9 Security concerns from data analysis for smart fridges.....	201
Table 6-10 Specific smart fridge guidelines	202
Table 6-11 Security concerns from data analysis for smart gateways.....	203
Table 6-12 Specific gateway guidelines.....	204
Table 7-1 Security concerns of IoT networks from a theoretical perspective	210
Table 7-2 Combined security threats from data	214
Table 7-3 Generic guidelines form literature.....	216
Table 7-4 Additional device specific guidelines from empirical study.....	217

CHAPTER 1 INTRODUCTION

1.1 INTRODUCTION

In just a few years, the internet has seen tremendous growth in devices that can interconnect, from the introduction of personal computers in the 80s to the birth of smartphones in 2007. Today we stand on the threshold of another internet revolution, the 4th industrial revolution, the Internet of Things (IoT) (Frangos, 2017). According to Antoniuk *et al.* (2017:262) the 4th industrial revolution is bridging the gap between cyberspace and physical space. By the year 2030, up to 500 billion devices will be connected to the internet (Cisco, 2019). These devices will be equipped with sensors, allowing them to be able to collect environmental data or any other type of data. Due to their network connectivity, these devices will be able to transmit collected data to servers in the cloud for analysis, which in turn will help these devices to make intelligent decisions or take better actions. Connected things fall under various categories, such as wearable devices, smart appliances, smart vehicles, smart buildings, and many more.

In the 4th industrial revolution or industry 4.0, machine to machine (M2M) protocol is vital to allow smart things to communicate with one another (Esfahani *et al.*, 2019:288). M2M communication will, for instance allow smart objects in a house to make intelligent decisions without user input. For instance, in a typical smart home, the nest thermostat in the house will detect when the owner leaves home and send a message to a washing machine which was busy. The washing machine will then change its set operation to longer cycles, which will result in energy saving (Miller, 2015:110). A door lock will be able to send a text message to the owner informing him when he forgot to lock it (Yale, 2019). In this dissertation a local area network is defined as a type of network that is limited to a certain geographic location (Clark *et al.*, 1978:1497; Teare, 1999:36). A home area network (HAN) is a local area network limited to a specific home.

Among the 500 billion devices which will connect to the internet by 2030, a portion of that number will comprise of household appliances, such as fridges, microwave ovens, stoves, coffee makers, air conditioners, electricity meters, televisions and many more. A number of these devices already have internet connectivity, such as smart televisions.

With such a high number of devices and home appliances connecting to the internet, security becomes a major concern for most homeowners. Unfortunately, with the rush to push more products onto the market, manufacturers of smart appliances have neglected the need for security as their priority (Green, 2015). The consequence of such an approach is a vulnerability to network attacks on data privacy which many homes have been exposed to. The study aims to identify the data security risk posed by current smart appliances and devices.

This chapter is structured into five sections. Section 1.2 describes the key concepts contained in the study. Section 1.3 describes the problem statement of the study. Section 1.4 presents the objectives of the study, including primary, theoretical, and empirical objectives. Section 1.5 describes the interpretive qualitative methodology used in the study with an emphasis on hermeneutics. Section 1.6 presents the ethical issues the study will abide by, followed by a presentation of the chapter classification in Section 1.7.

1.2 CONCEPTS KEY TO THE STUDY

Home area networks (HANs) are part of the phenomenon of “Internet of Things”, thus it is imperative that a common understanding of these concepts is created.

1.2.1 Internet of Things

Gartner (2019) defines Internet of Things (IoT) as “*the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or external environment.*” Application areas of IoT varies from industrial, medical, military, to home automation. A number of home devices come with network connectivity, such as smart televisions, fridges, air conditioners, washing machines, smart cameras, smart locks, smart speakers, water leakage detectors and many more. Most of these devices need electricity to operate, while some devices operate on batteries. For such devices, there is a need for a better wireless communication protocol which is power efficient, such as ZigBee, Z-Wave (Al-Sarawi *et al.*, 2017:685), or any other low energy protocol. For devices such as water leakage detectors, or smart locks, which operate on batteries, a low energy communication protocol is vital. Many IoT devices in a home area network connect to a central device called an IoT gateway or informally called a hub (Britt *et al.*, 2017). An IoT gateway interconnects many IoT devices using different communication

protocols, allowing them to communicate with one another. The gateway may also provide internet connectivity to these devices. Internet connectivity to IoT devices enables one to control these devices over the internet. Chapter 3 presents an investigation of IoT literature.

1.2.2 Network Security

Network security involves protecting a computer network from threats that may originate within or outside of the network. Many high-end devices such as computers, smartphones, and tablets do come equipped with an operating system which has security features, such as built-in encryption (Bruni *et al.*, 2014:108). The hardware, such as the amount of RAM and CPU speed, is more than enough to run resource-intensive applications such as antivirus software. Unfortunately, the majority of IoT devices do not possess the processing power required to run applications which allows it to detect vulnerabilities, or even encrypt the data which they generate.

How can someone detect whether his smart fridge has been infected with malware? The limited processing power of most of these devices, as well as their ability to connect to the internet, make them a security risk for any household. Security is a layered approach (Dube & Ramanarayanan, 2004). In a home area network, security can be applied to the network level as well as device level. Many devices come with default security settings, and many people, due to lack of information, connect these devices to the internet with those settings opening up a whole world of vulnerabilities on the network. A network that is not properly secured will result in the privacy of the home being compromised. Network security is discussed in Chapter 4.

1.2.3 Data Privacy

In this digital age, people's lives exist in the digital space. It is possible to learn enough about a person by just looking at their digital profiles (Fertik, 2012). The majority of this data is put there voluntarily by the users themselves. However, when it comes to someone's home, privacy takes on a whole new meaning. No one would like information collected about them without their permission, which is exactly what is happening with most smart devices. Let us consider for example smart electricity meters, the data generated by these meters is normally transmitted to the utility company every 30 seconds; and most of the time this information is not encrypted. The utility can be able to have a better understanding of energy usage. The data also can enable a family to better manage their electricity usage. Although these are all great benefits on both sides, there

have been major concerns about the data transmitted by these meters (IBT, 2012). For instance, the data collected can easily reveal when people are home and when they are not, making it easy for a thief to break in. The fact that kill switches are incorporated in these meters, make them even more dangerous in the wrong hands. Imagine if the system can be hacked, energy supply can easily be switched off remotely causing great havoc (Peev, 2012). Although such devices can greatly improve people's livelihood, the concern over data privacy cannot be overlooked. Privacy concerns are discussed as part of network security in Chapter 4.

1.3 PROBLEM STATEMENT

With an increasing number of common household appliances connecting to the internet, our homes are no longer a private/secure area. The majority of home appliance stores in South Africa are already full of internet-ready devices such as smart TVs. As these devices connect to the internet and are able to collect user data and transmit it over the internet, these devices become a portal to unintentional data privacy issues in our homes.

1.4 OBJECTIVES OF THE STUDY

The primary objective of this study is to identify the security threats which smart home devices may pose to unsuspecting homeowners concerning their data privacy.

This primary objective is developed into theoretical and empirical sub-objectives as described below.

1.4.1 Theoretical sub-objectives

The theoretical objectives are achieved by reviewing literature and are formulated as:

1. To investigate and justify the selection of a suitable research methodology for this study;
2. To demonstrate an understanding of smart devices in terms of hardware, software and network connectivity;
3. To demonstrate an understanding of security threats posed by smart devices to data privacy in home area networks from a computer security literature perspective.

1.4.2 Empirical sub-objectives

The empirical sub-objectives are used to guide the data collection and analysis process and are formulated as:

1. To collect data from manufacturers' technical documents and reviewers' documents on specific smart devices such as smart televisions, speakers, locks and fridges;
2. To compare and analyse the two data sources and literature in order to identify data privacy threats for these devices.
3. To develop guidelines for unsuspecting homeowners in relation to their privacy in home area networks, to consider when selecting smart devices.

The next section considers research methodology matters used in this study.

1.5 RESEARCH DESIGN AND METHODOLOGY

A brief introduction to research design and methodology is given in this section, with more detailed coverage of the topic provided in Chapter 2. A literature study is conducted on the key concepts introduced in this chapter using books, and peer-reviewed articles. Secondary data sources include: Internet articles, technical documents, and security policies. The empirical study is introduced here in terms of paradigm, principles and method.

1.5.1 Research paradigm

They are four widely used research paradigms in information systems research, namely, positivism, interpretivism, critical social theory (Klein & Myers, 1999:24), and design science research (Gregor, 2006:614). These paradigms are based on distinguishable ontological and epistemological assumptions. *Positivism* is based ontologically on realism and epistemologically on objective repeatable knowledge. Positivistic studies usually make use of quantitative data collection and analysis techniques (Meyers, 2015).

Interpretivism is based on the ontological assumption of relativism. In interpretive research, knowledge of reality is obtained only through social construction, such as documents, language, and other artefacts. Interpretivism attempts to understand phenomena through the meanings which people assign to them (Bowen, 2009:29). Qualitative data collection and analysis techniques are mostly associated with this paradigm.

Critical social theory aims at emancipating a subject from a situation of alienation and oppression (Bowen, 2009:29). Theories are developed through participative change and the reflection thereupon.

Design Science Research aims at creating new knowledge through the creation of artefacts. These artefacts can be constructs, techniques, or methods (Vaishnavi & Kuechler, 2004:49) and knowledge is created through reflection on the artefact design and development processes.

In this study, we have taken an interpretive stance because our aim is to identify security threats in home area networks and to understand their impact on data privacy from various perspectives. The study is not positivist since it values the subjective perspectives of reviewers of devices. The main aim of the study involves understanding and although emancipation might be achieved as a result of the study, the epistemological assumption is to develop a theory from data rather than theory from change. It is therefore not in the critical social theory paradigm. The design science research paradigm is not applicable to this study since it is not focussed on artefact development. A more detailed justification for choosing interpretivism is provided in Chapter 2.

1.5.2 Principles of interpretive research

Since the interpretive paradigm is used in this research, the principles developed by Klein and Myers (1999:24) for conducting interpretive research in information systems are used to guide the research. The application of the principles is briefly reported here, while their theoretical meaning is discussed in Chapter 2:

1.5.2.1 *The fundamental principle of the hermeneutic circle*

To understand the security threats posed by smart appliances in a home area network, the researcher investigates the security of each individual smart appliance and reflect on how they affect the security of the home area network as a whole, as well as the security threats posed by the connection of these devices.

1.5.2.2 *The principle of contextualization*

The research needs to take into consideration the context of reviewers, researchers, and device manufacturers as to the motives behind their comments or reviews.

1.5.2.3 *The principle of interaction between the researcher(s) and subject*

Although the researcher may not be able to interact with the participants, as in the case of this research, the researcher's biases can still affect the consideration of the material. Hence the researcher should also evaluate and state his stance on the research problem.

1.5.2.4 *The principle of dialogical reasoning*

Should the researcher have any biases during the course of the study, he would need to confront his biases, should the results prove otherwise.

1.5.2.5 *The principle of multiple interpretations*

With data collected from multiple online documents, it is important that the researcher analyses documents from different sources to avoid or eliminate contradictions which may exist.

1.5.3 Research Methods

Research methods direct a researcher on data collection or data analysis methods. The following two sections describe the data collection and analysis methods adopted in this research.

1.5.3.1 *Data collection*

Document analysis is part of an online qualitative research methodology which focuses on analysing data contained in online documents, consumer reviews, such as news articles, blogs, or scientific articles. In this study, two types of data sources are used. The first source of data is technical documents of devices published by the manufacturers. The second data source is online documents such as blogs, news articles, white papers and product reviews. Due to the specific aim of the study, the focus is not on interviewing people. Sometimes documents may become the only source in interpretive research of hermeneutic nature (Bowen, 2009:29). Document analysis is used to analyse online documents.

1.5.3.2 *Data analysis*

Document data analysis is based on interpretive content analysis methods. Coding is used to generate a theory that fits the data. Coding involves attaching labels to pieces of text which are relevant to a particular idea which is of interest in the study. Codes are then combined to form themes representative of the data (Meyers, 2015). Chapter 2 provides a theoretical foundation for the methods used in the study.

1.5.4 Rigour and evaluation of methods

Since people such as reviewers and manufacturers may have hidden agendas behind their writing, it is important that the information is scrutinised to eliminate any biases that may exist on the writer's part. The empirical report includes all data required to trace the flow of the argument. Care is taken to present findings in a manner which is traceable to the source documents.

1.5.5 Delimitations to the study

The initial delimitations of the study can be linked to five aspects:

- No interviews are to be conducted. The aim is to identify threats from the technical specifications of the devices rather than from the experiences of users. Data collection rely on manufacturer's manuals and review documents.
- No appliances are available to test physically due to financial constraints.
- Due to the frequent release of new appliances, there might be newer appliances available than the ones discussed. In selecting a specific model to investigate, the number of available reviews and the market share are considered.
- Documents posted on the internet are updated frequently, this is a substantial challenge in this study. From this perspective, this study can never be inclusive of all the documents sited, as these documents might have changed after use by the researcher.
- Laptops, personal computers, tablets and mobile phones are not explicitly part of the study beyond the applications loaded on them to control smart devices and appliances.

The limitations are reflected upon in the final chapter of the study.

1.6 ETHICAL CONSIDERATIONS

The following ethical considerations are be taken into account:

- To ensure the information used is found in the public domain;
- To adhere to the ethics guidelines for studies at the NWU where the student is registered.

1.7 CHAPTER CLASSIFICATION

This study comprises the following chapters:

Chapter 1 Introduction and background to the study:

This current chapter provides an introduction to the study, covering information on the motivation of the project as well as the objectives the study.

Chapter 2 Research design and methodology:

This chapter provides detail of the research methodology used in the study uses to achieve its objective. Interpretive qualitative methodology is the preferred methodology of the study, with emphasis on data collection and analysis from documents.

Chapter 3 & Chapter 4 Literature review:

A literature review provides a detailed explanation of the principle research concepts undertaken in this study. Areas of review include the IoT, smart devices, device connectivity, network security, and data security.

Chapter 5 Results and findings:

This chapter presents the data collected and demonstrates the analysis process. It presents findings from data for the study grounded in the data collected and analysed.

Chapter 6 Guideline development

This chapter presents the integration of the literature insights with the findings from the empirical data. The chapter presents guidelines for home owners to consider when selecting and using smart devices in their home area network.

Chapter 7 Summary and conclusions

This chapter presents the summary of the study as well as the final conclusion. It includes an evaluation of the study and concludes with a reflection on future research.

1.8 CHAPTER SUMMARY

This chapter has laid the foundation of the research work reported in this dissertation. With an increasing number of common household appliances connecting to the internet, our homes are no longer a private/secure area. The focus this research focuses on are IoT technology, network security and data privacy. The primary objective of this study is to identify the security threats which smart home devices may pose to unsuspecting homeowners concerning their data privacy.

The objectives of the research are divided into two groups, theoretical and empirical. The theoretical objectives are accomplished by means of a study of IoT components and network security in Chapter 3 and Chapter 4. Theoretical understanding is then enhanced by an empirical investigation of internet documents, presented in Chapter 5.

The first theoretical objective on the selection and justification of an appropriate methodology the concern of next chapter.

CHAPTER 2 RESEARCH METHODOLOGY

2.1 INTRODUCTION

The primary objective of this study is to identify the security threats which smart home devices may pose to unsuspecting homeowners concerning their data privacy.

The objective of this chapter is to review the various research approaches which are available, in order to justify the selection of the research approach best fit for this study. Amaratunga *et al.* (2002:17) define research as “a systematic and methodical process of enquiry and investigation which result in an increase in knowledge”. They further discuss six conditions that research should satisfy:

1. It must be an orderly investigation of a defined problem.
2. Appropriate scientific methods need to be used.
3. Adequate and representative evidence need to be gathered.
4. Logical reasoning, uncoloured by bias, needs to be employed in drawing conclusions on the basis of the evidence.
5. The researcher is able to demonstrate or prove the validity or reasonableness of their conclusions.
6. The cumulative results of research in a given area yield general principles or laws that may be applied with confidence under similar conditions in future.

Before data can be collected, it is important to first establish the research philosophy. Saunders (2011:106) compares the steps research must go through to the layers of an onion. Just as onions need to be peeled off to get to the inner layers, so are the steps involved in the research. Data collection is one of the inner layers, thus to get to it, it is important to understand the outer layers.

This chapter is structured as follows, in Section 2.2 various research paradigms are discussed, in Section 2.3 a more detailed discussion of interpretive research methodologies is given, in Section 2.4, a discussion of various interpretive research designs is provided. Section 2.5 briefly compares

qualitative and quantitative method, followed by a description interpretive data collection method in Section 2.6. Section 2.7 provides a discussion of different qualitative data analysis methods. In Section 2.8 the research plan is laid out, and finally, Section 2.9 summarises the chapter.

2.2 RESEARCH PARADIGMS

Research philosophy which is embodied in research paradigms involves the development of knowledge and the nature of that knowledge (Saunders, 2011:107). When one embarks on research, the aim is to develop new insights which will help in answering the research question. Each research paradigm is defined by two significant assumptions, its ontological and epistemological assumptions.

- I. *Ontology*: Ontology describes the nature of reality or theories of what exists (Rawnsley, 1998:2; Saunders, 2011:110). The ontological assumption answers the question of “what is a reality?” for example, the ontological assumption of realism is that the world exists outside and independent of the observer. The ontological assumption of relativism is that reality depends on the observer. Reality does not exist; it is constructed via the perception of the observer (Saunders, 2011:114-115). For example, if a black car was parked in a parking lot outside, two individuals looking at the same car from different angles and light perspectives may see different colours. One may see the car looking greenish, if the paint has a tint of green in it, the other may see it as black. From this example, the realities of these two observers will not be the same; it will be dependent on what the observer perceives. The ontological assumption of critical social theory is that “people are the creators of their social world, and as such, can change it if they wish.” (Ngwenyama, 1991:2). The observer does not just accept reality as it is, but can reason, question, and even offer a better alternative. For instance, in the example of the black car parked in a parking lot, to a critical theorist, he will accept the reality that the car is black, but he will go further to reason as to why the car is black in the first place and not another colour.
- II. *Epistemology*: Epistemology is concerned with what constitutes what is adequate knowledge in the area of study. Epistemological assumptions answer the question of “where is the source of knowledge?” (Saunders, 2011:112). In the various research

paradigms that exist, knowledge can be created using a number of methods. For instance, positivists formulate a hypothesis for a problem. We can think of a hypothesis as a statement without proof, so data may need to be collected through experiments to prove or refute the hypothesis. Interpretivist researchers on the other hand may use various methods to obtain data and then develop a theory from the data. For instance, in ethnography a researcher may live among a group of people and observe how they do certain things, thus gaining knowledge of their social life. On the other hand, with critical social theory, knowledge is obtained through emancipation (Dieronitou, 2014:7).

Various research paradigms can be differentiated by examining their ontological and epistemological stances (Walsham, 1995:75). In the following section, four main paradigms are discussed. These include positivism, interpretivism, critical social theory, and design science research.

2.2.1 Positivism

Positivism, ontologically, falls in the realm of realism. Epistemologically, positivism makes use of hypotheses. Hypotheses are created and tested, in whole or in part, and can be supported or refuted (Saunders, 2011:113). More data¹ are then gathered to prove the hypothesis further; this is known as deductive research. In interpretive studies (discussed in the next section), data are collected first, and theories are created later to describe the data, this process is known as inductive research (Sekaran, 2006:31).

Research projects may be categorized as positivistic mainly based on the data collection methods they employ. Positivistic studies are known to make use of the following three data gathering methods: experiments, surveys, and field studies (Weber, 2004:10). Objectivism is inherent to positivistic methods. The objective assumption is that a researcher is independent of and can neither affect or be affected by the subject of the research (Saunders, 2011:114).

2.2.2 Interpretivism

¹ Data collected for research are treated as plural in this chapter (and next two chapters). This is in contrast to data in the computer industry that is treated as singular according to the collective noun rule.

Interpretive research is used by researchers who want to understand human thoughts and actions in social and organizational contexts (Klein & Myers, 1999:67). According to Saunders (2011:116), interpretivism promotes the importance for researchers to recognize the variance between humans in our role as social players.

Ontologically, interpretivism falls into the realm of relativism. Unlike positivists who believe in only one reality, the goal of interpretivism is to understand different realities. Epistemologically, with interpretivism, researchers gather data first then create a theory or an abstraction to be tested by further data collection. More and more data are collected to strengthen the theory. The data are collected incrementally. If collected data do not fit proposed theory, the theory is refined and the process continued until saturation is reached.

Interpretive research methods include case studies, ethnography, phenomenography, and ethno-methodological studies. Unlike positivistic researchers who conduct the data collection objectively, the nature of interpretive research means that the researchers themselves will become measurement tools, in that researchers can interpret the phenomenon they observe subjectively (Weber, 2004:7).

2.2.3 Critical social theory

Critical social theory is defined by Leonardo (2004:11) as a “multidisciplinary framework with the implicit goal of advancing the emancipatory function of knowledge.”. Critical social theory can also be thought of as a way to initiate social changes by exposing the inequalities which may exist in a society (Rush, 2006:9). While traditional social theory focuses on understanding and analysing the status quo, critical social theory, on the other hand, is concerned with finding favourable social conditions in comparison to the existing ones (Ngwenyama, 1991:2).

According to Dieronitou (2014:7), “the ontological assumption which underpins critical social theory is that of critical realism”. Critical social theory is satisfactory only if it meets the ensuing three conditions simultaneously, that is, it has to be explanatory, it has to be practical, and lastly it has to be prescriptive (Bohman, 2005).

From the explanation above, it follows that the epistemological assumption of critical social theory is that, knowledge is created via emancipation. To be able to achieve emancipation, it is required

to deconstruct reality to identify oppressive structures. Then we can reconstruct reality without these oppressive structures (Leonardo, 2004:12).

2.2.4 Design Science Research

According to Blessing and Chakrabarti (2009:1), “the aims of design research are the formulation and validation of models and theories about the phenomenon of design, as well as the development and validation of knowledge, methods and tools – founded on these theories – to improve the design process.”

The evolution of design science research (DSR) has even seen the name change from design research (DR) to DSR. The main differences, according to Vaishnavi and Kuechler (2004:6), is that DR focuses on the design, on the other hand, DSR is mainly concerned with research which uses design as a research method.

The end results of DSR are “social-technical artefacts” (Gregor & Hevner, 2013). These artefacts may include “decision support systems, modelling tools, governance strategies, methods for IS evaluation, and Information System (IS) change intervention.”

According to Vaishnavi and Kuechler (2004:21), the metaphysical assumptions of DSR are unique for two prime reasons. First, none of the ontology or epistemology assumptions of DSR paradigm is derived from any known paradigms. Second, with DSR the ontological and epistemological assumptions change through the course of a project. Ontologically, “DSR researchers believe in a single, stable underlying physical reality that constrains world-states” (Vaishnavi & Kuechler, 2015:31). Epistemologically, in DSR knowledge is created via the design of artefacts (Hevner & Chatterjee, 2010:1).

Artefacts created in DSR need to fulfil two vital characteristics. First, they need to be able to solve important problems which are relevant. Second, they need to clearly differentiate between DSR and other routine designs. Thus, DSR should be able to address an unsolved problem in either a unique and innovative way or a solved problem in a more effective and efficient way (Geerts, 2011).

2.2.5 Position of this study

The position of the researcher in this study is not objective since he needs to identify with subjective views in order to understand the perceived risks. No hypothesis will be formulated in this research; hence it will not be positivist in nature. The critical social theory will also not be adopted because emancipation is not explicitly part of the research process. DSR will not be used because no artefact is being created. The researcher will take an interpretive stance because the aim of the research is to identify security threats in home area networks and to understand their impact on data privacy from various perspectives. Epistemologically, the research will gather data from published documents in support of theory development. Ontologically, the research will attempt to understand the reality of what is being studied by means of the interpretation of the different perspectives.

2.3 INTERPRETIVE RESEARCH METHODOLOGY

Interpretive researches practices are mainly used with interpretive methodologies. Klein and Myers (1999:63-93) discuss a set of principles which each interpretive researcher should follow when conducting an interpretive case study. These principles are not rigid prescriptions, rather Klein and Myers (1999:71) explain that each researcher should evaluate and ascertain which of these principles apply to their research.

With every research project, there are guidelines that direct the researcher in the way he/she should carry out his/her research. These guidelines help to ensure certain standards are followed. In this section, seven guidelines or principles of conducting an interpretive case study research, are discussed.

2.3.1 The fundamental principle of hermeneutics

The key to interpretive research methodology, is the principle of hermeneutics. Hermeneutics is concerned with the process of the creation of interpretive understanding (Boell, 2010:132). Fundamental to the principle of hermeneutics is the hermeneutic circle. The idea behind the hermeneutic circle is that for us to understand the whole, we need to understand the parts, and for us to understand the parts we need to understand the whole (Klein & Myers, 1999:71). For instance, to understand security in a smart home (*the whole*), we need to look at the security

implementation of each device; and for us to understand how each appliance and device affect the security of a smart home, we need to look at network security in a smart home as a whole.

2.3.2 The principle of contextualization

According to Klein and Myers (1999:73), the principal of contextualization is based on Gadamer's understanding, that there exists a fundamental difference in understanding between the author of a text and the interpreter, due to the distance between them. Klein and Myers (1999:73) describe the primary task of this principle as one of seeking meaning in the context. Thus, conceptualization requires that the issue being researched, be set in its social and historical context so that the targeted addressees can observe how the existing condition under study came about (Klein & Myers, 1999:73). This principle applies well to this research. Through the analysis of many documents on privacy policies of the various appliances under study, it is important to understand the context of some statements made in these documents. For instance, in one of Samsung's privacy policy documents, it was stipulated that they do collect even sensitive data through their smart TVs. It is important to try and understand the context of their statement.

2.3.3 The principle of interaction between the researcher and the subjects

This principle requires that both the researcher and the participants be placed into a historical perspective. Thus, the data collected is as the result of the interaction between the researcher and the participants. In this way, both interpretive researchers and the participants can be viewed as interpreters and analysts (Klein & Myers, 1999:74). Although no direct participants will be involved in this study, this principle does apply to this research therein that the data collected via documents, such as online reviews, is considered as interviews with participants.

2.3.4 The principle of abstraction and generalization

Abstraction is described as the "process of initial concept formulation and generalization of ideas by extracting common qualities from specific examples." (Klein & Myers, 1999:75). They also emphasize the importance of a relationship between theoretical abstraction and generalization. The aim of this relationship is to help readers understand how the researcher arrived at his conclusion. In this study, this principle will be applied by analysing the data in order to formulate the findings.

The analysis is an ongoing process and implementation of the hermeneutic cycle. This will help readers to understand how the theory was developed in a systematic, auditable manner.

2.3.5 The principle of dialogical reasoning

As a researcher, we have a priori theory that we would like to prove, right through our findings. At times though, the data collected may prove our theory to be wrong. Following the principle of dialogical reasoning as a researcher, the researcher will have to reconcile the preconceptions that guided the original research question (Klein & Myers, 1999:82). For instance, the *a priori* theory is that the introduction of smart appliances into smart homes will compromise the privacy of homeowners. This theory may be impossible to substantiate from the data collected in this study.

2.3.6 The principle of multiple interpretations

This principle shows that research participants may have different interpretations of the same finding, as Klein and Myers (1999:83) shows. For instance, data collected may prove that smart appliances introduce security weaknesses into a HAN due to their lack of built-in security, but a specific reviewer may give a different interpretation.

2.3.7 The principle of suspicion

The purpose of this principle is to unveil the effect of distortion introduced by the participants (Klein & Myers, 1999:77). Whereas the other six principles focus on the interpretation of meaning, the principle of suspicion focuses on the discovery of false preconception (Klein & Myers, 1999:77). Since data are collected from online reviews, it is important that this principle is applied to ensure that no false information is collected.

The next section describes possible overall research designs which can be used to practise these principles.

2.4 INTERPRETIVE RESEARCH DESIGNS

The role of the researcher in interpretive data collection is that of a participant. The researcher enters the research setting in various ways. Saunders (2011:136-167) discusses the following possibilities: case study and ethnography. Myers (1997:6) argues that action research can be done

from an interpretive perspective and the discussion is extended to include archival research as candidate design.

2.4.1 Case study

A case study is defined as “a strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real-life context using multiple sources of evidence” (Saunders, 2011:146). A case study can be used in various interpretive research methods, but in each of these methods the context will be different. Gerring (2006:21) goes further by defining what a case is and how it applies to different research methods. He defines a case as “a spatially delimited phenomenon (or unit) observed at a single point in time or over some period of time.” He explains how each case will be different based on the field one is researching on. For instance, in a study where the researcher is trying to explain the behaviour of people, as in clinical psychology, his case will comprise of individuals. On the other hand, for a researcher doing a study in social-political science, his case may comprise of cities, communities, political parties, etc. Thus, in each of these examples, a case may provide a single observation or multiple observations, according to Gerring (2006:21). Data collection methods used in interpretive case studies may include interviews, focus groups, and data from documents. (Darke *et al.*, 1998:282).

2.4.2 Action research

Greenwood and Levin (2006:16) define action research as “social research carried out by a team that encompasses a professional action researcher and the members of an organization, community, or network “stakeholders” who are seeking to improve the participants’ situation.”

They further explain that with action research, the researcher and the stakeholders, independently defines what the issue to be solved is, then work together to generate essential knowledge concerning this issue, learn and execute social techniques, take actions, and interpret the results of the measures based on what they have learned. Saunders (2011:147) also adds, that action research can involve the process of diagnosing, planning, taking action and evaluating as shown in Figure 2-1.

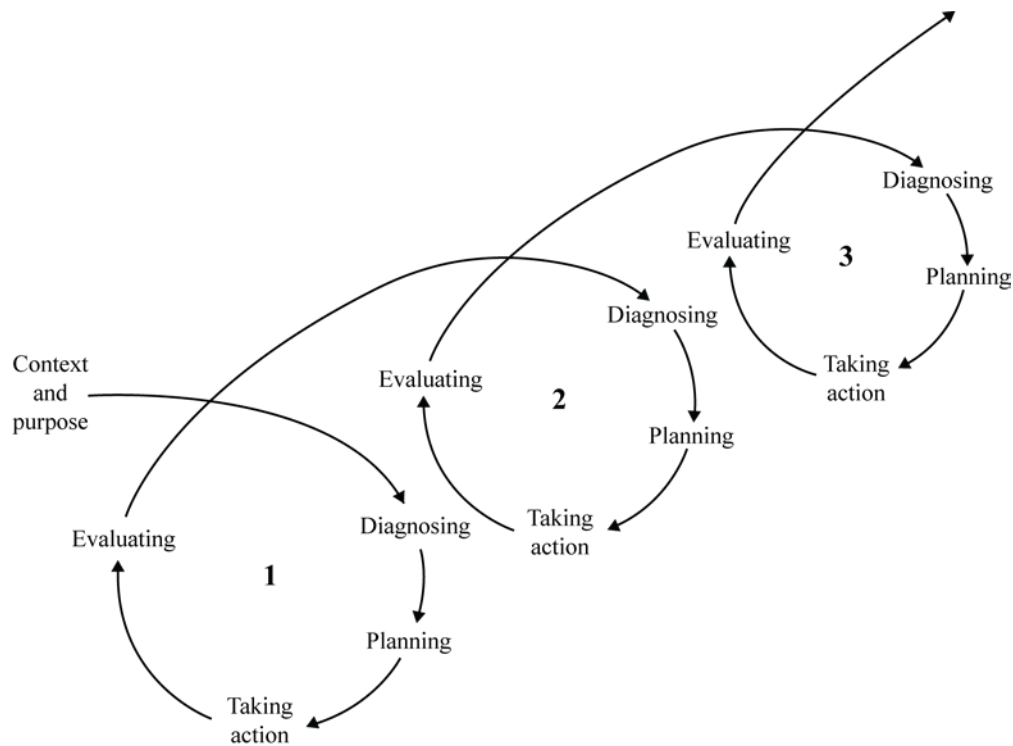


Figure 2-1 Action research spiral adapted from Saunders (2011:148)

As shown in Figure 2-1, the process of doing research using AR becomes an iterative one. The process starts with a problem to be solved (context). The diagnosis step may involve some fact-finding processes on the issue at hand. Then action planning and decisions taken, need to be evaluated. The results from the subsequent cycle are again put through the same steps in a different cycle where further diagnosis, planning, taking action, and evaluation are considered again. The process is repeated again and again until a solution is obtained. Action research may be performed from positivist, interpretive, or critical social theory perspective (Klein & Myers, 1999:68).

2.4.3 Ethnographic research

Ethnographic research focuses on explaining the social world by a researcher in a way that the subject being studied would have explained it him/herself (Saunders, 2011:149). This involves the researcher living among a group of people or in a society to better understand firsthand and feel what the subjects being studied are going through, this is known as participant observation. Wortham (2010:1) gives a shorter definition of ethnography as *“the study of culture and social organization through participant observation and interviewing.”*

Interviews though might not bear much fruit if the subjects being studied are total strangers. Living with the subjects, helps in making sure if interviews are ever needed, the subjects will be open to talking. If interviews are ever used, the whole process should be as natural as possible (Swanson & Holton, 2005:283). Ethnography, with its roots in anthropology, has been used by many researchers to study the behaviour and lifestyle of communities as well as to study an exotic tribe living in remote places. In most of these instances, researchers are known to have spent months or even years living as part of the community to better understand the subjects. Thus ethnography is known to be a time-consuming process. Data collected from such research may include artefacts, photos, songs, documents, etc. (Swanson & Holton, 2005:283).

2.4.4 Archival research

Archival research is a research practice that involves the use of administrative records or documents as a source of data (Saunders, 2011:150). What is considered as an archive? Archives can include any collection of historical data, among which can be, company memos, letters, technical manuals, training manuals, etc. It can also include photos and videos. Instead of archives just being viewed a collection of historical data stored somewhere in the basement, according to Gaillet *et al.* (2012:39), archives are now being considered as the primary source for creating new knowledge. Saunders (2011:150) further elaborates on archives, by pointing out that when archives are used in archival research, they become a “product of day-to-day activities”. Thus, these archives become “part of the reality being studied” rather than just being a collection of historical data. Archives are not only confined to a library or an archival room in a museum, a number of digital archives are readily available on the internet. Not only do Web 2.0 based digital archives allow researchers to carry out their research by accessing artefacts which are available online, but they also allow users to contribute to these archives (Purdy, 2011:34). Thus today, the web is viewed as “the most important archive ever created” (Gaillet *et al.*, 2012:38).

This research study is conducted as a case study using data from documents. The data used are not considered archives. Archives implicates that the data were in an operational system and then stored as historical data, which is not the case for the data used in this study.

2.5 QUALITATIVE VERSUS QUANTITATIVE RESEARCH

Traditionally research methodologies have always fallen into two groups, either quantitative or qualitative (Amaratunga *et al.*, 2002:19). The distinction between these two methodologies has led to disputes in the past, resulting in two camps of purists, respectively for quantitative and qualitative methodologies (Johnson & Onwuegbuzie, 2004:14).

According to Bryman (2006:112), qualitative and quantitative research refer rather to techniques or methods used to collect data and the approach taken to analyse such data. Seaman (1999:557) describes qualitative data as data represented in words and pictures but not in numbers. Qualitative data can be collected using methods such as interviews, participants observation, or questionnaires (Seaman, 1999:557). According to Darke *et al.* (1998:275), qualitative methods focus mainly on words and meanings.

On the other hand, methods used to collect quantitative data focus on “observation and measurements of reality” (Trochim & Donnelly, 2001:22). Quantitative data are mainly numerical data obtained from controlled experiments (McLaughlin *et al.*, 2016:716).

Depending on the researcher’s paradigm, one can choose either method or can combine both in a single study. As Klein and Myers (1999:69) shows, qualitative methods may or may not be interpretive in nature, it will depend on the philosophical assumption of the researcher. It is true that coded qualitative data can be transformed into quantitative data, and quantitative data can also be converted into qualitative data. Driscoll *et al.* (2007:20) describe the two processes as “*quantitizing*” and “*qualitizing*”. In this dissertation, an interpretive stance to qualitative data collection method is adopted.

Qualitative methods help to answer the question “why?” offering insight into people’s behaviour. For instance, it may provide answers to why people act and behave in certain ways (Rosenthal, 2016:509). Common qualitative data collection methods discussed in the next section, include interviews and participant observation (Wohlin & Aurum, 2015:1437).

2.6 QUALITATIVE DATA COLLECTION

In this section applicable methods for collecting qualitative data from an interpretative perspective are discussed including interviews, grounded theory, and document research.

2.7 QUALITATIVE DATA ANALYSIS METHODS

Data collection methods in qualitative research can generate a large amount of data according to Pope *et al.* (2000). The data may come from “transcripts of unstructured interviews, field notes, documents, diaries or life stories” (Life, 1994:59). For this data to be useful, it needs to be analysed so that it can be understood. In the process of doing this analysis, a theory may be developed from the data (Saunders, 2011:480). An approach to data analysis methods can either be inductive or deductive (Pope *et al.*, 2000). In an inductive approach, such as used in grounded theory, one start by collecting data and then explore the data to identify which themes to follow up and focus on them (Saunders, 2011:490). Hyde (2000:83) defines inductive reasoning as “*a theory testing process, starting with observations of specific instances, and seeking to establish generalizations about the phenomenon.*” Whereas he describes deductive reasoning as “*a theory testing process, which commences with an established theory or generalization, and seeks to see if the theory applies to specific instances.*” Framework approach and thematic analysis are two methods that make use of a deductive approach (Smith & Firth, 2011). The approach adopted in this dissertation is deductive in nature, since documents as are used in support of a theoretical investigation.

According to Smith and Firth (2011:3), there are three methods through which data analysis method can be conducted: “

- Socio-linguistic methods that explore the use of the meaning of languages such as discourse and conversation analysis;
- Methods that focus on developing theory, such as grounded theory;
- Methods that describe and interpret participants’ views such as content and thematic analysis.”

In this dissertation content analysis, as socio-linguistic method, has been selected as the preferred data analysis method since the source of data to be analysed comes from documents. Section 2.7.2 discusses in detail content analysis as a data analysis method.

2.7.1 Grounded theory

In Section 2.7.4 grounded theory is discussed as a methodology that can be used to generate theory in terms of data collection. Another aspect of grounded theory is that of being used as a data analysis method in interpretive research as discussed by Heath and Cowley (2004:141-150). Urquhart *et al.* (2010:361) describe grounded theory as a qualitative research method for gathering and analysing data. According to Corbin and Strauss (1990:6), when grounded theory is used, analysis of data starts immediately once the first bit of data has been collected. This is different from positivistic methods where all the data are collected before the analysis process starts. They argue that doing analysis from the start is vital because it helps in guiding what is next when conducting an interview or an observation. Thus according to Urquhart *et al.* (2010:357), the interchange between data collection and analysis is vital throughout the whole process. They argue that data collection, analysis and coding should be carried out as one unit because their interaction is fundamental to grounded theory. This iterative process is demonstrated in Figure 2-2.

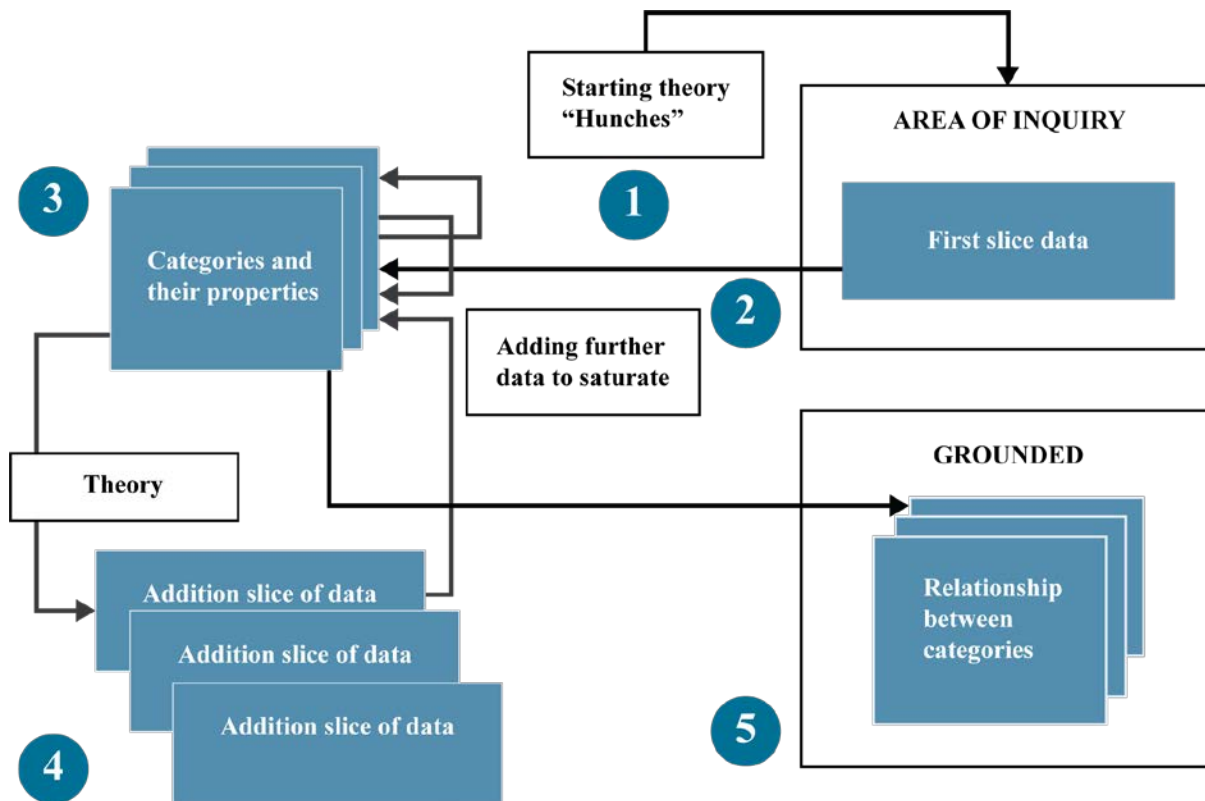


Figure 2-2 Cycle of data collection and analysis in grounded theory adapted from Urquhart et al. (2010:363)

Grounded theory starts with an assumption or a theory that is based on a hunch for investigation (Urquhart et al., 2010:362), as shown by step one in Figure 2-2. The source of these preconceived theories may come from other sources than the data itself. In step two, a slice of data is taken from the area of inquiry and coded into concepts as shown in step 3. Concepts that belong to the same phenomenon can then be grouped into categories (or conceptual categories). Concepts are the building blocks of analysis in grounded theory (Corbin & Strauss, 1990:7).

In step three, the conceptual categories are then compared with each other and their relationships. In step four, more slices of data are taken until the categories are saturated. According to Kendall (1999:746), conceptual saturation is reached “when no more new categories are generated from open coding, and the remaining gaps in the emerging scheme are filled”. In step five, it is the integration of the conceptual categories and their interrelationships, especially with the core categories, that lead to grounded theory (Kendall, 1999:746).

2.7.1.1 *Coding*

Coding can be described as the process of “transforming raw data into theoretical constructions of social processes” (Kendall, 1999:746). Corbin and Strauss (1990:12) though, think of coding as data analysis process. According to Kendall (1999:746), through the process of emergence, codes and categories should be able to fit the data. She argues that this fitting of data should not fit to a predetermined code and categories. She further states that code and categories should not be created before the data analysis process, they should rather emerge from the words found in the data.

Due to the diversity in coding procedures, Glaser (Kendall, 1999:746) describes two types of coding, whereas Corbin and Strauss (1990:12) describe three types of coding, open, axial, and selective. In this section, Corbin and Strauss’ explanation of coding is adopted.

- I. *Open coding*: Open coding is described as the process of breaking data analytically, with the purpose of giving the researcher new understanding, by “breaking through standard ways of thinking about or interpreting phenomena reflected in the data” (Corbin & Strauss, 1990:12).
- II. *Axial coding*: In axial coding, “categories are related to their subcategories and their relationship is tested” (Corbin & Strauss, 1990:12). Axial coding is described as “a set of procedures whereby data are put back together in new ways after open coding, by making connections between categories. This is done by using a coding paradigm involving conditions, context, action/interactional strategies, and consequences” (Kendall, 1999:747).
- III. *Selective coding*: Selective coding is a process that systematically relates the core category to other categories and integrates and refine the categories into theoretical constructions (Kendall, 1999:747). According to Corbin and Strauss (1990:14), the core category represents the central phenomenon of the study, and it can be identified by asking questions such as: “What is the main analytic idea presented in this research?”.

Open coding as described in grounded theory is foundational to other qualitative data analysis methods, including content analysis.

2.7.2 Content analysis

Content analysis is defined by Vaismoradi *et al.* (2013:400) as “*a systematic coding and categorizing approach used for exploring a large amount of textual information unobtrusively to determining trends and patterns of words used, their frequency, their relationship, and the structure and discourse of communication*”. Elo and Kyngäs (2008:107) define content analysis as “a method of analysing written, verbal or visual communication.” This definition is supported by Stemler (2001:1), who argues that content analysis is not limited only to text, but can also be used to code drawings. If text is the focus of analysis, this may be obtained in printed, verbal, or electronic format. The sources of these may include open-ended survey questions, interviews, focus groups, observations, or printed media such as articles, books, or manuals (Hsieh & Shannon, 2005:1278).

According to Stemler (2001), every researcher embarking in content analysis should review the following six questions “

- Which data are analysed?
- How are they defined?
- What is the population from which they are drawn?
- What is the context relative to which data are analysed?
- What is the boundaries of the analysis?
- What is the target of interest?

Content analysis can be either qualitative or quantitative in an inductive or deductive way according to Elo and Kyngäs (2008:113). An inductive approach to data analysis can be employed when there is not enough information about a phenomenon, or if the current information is fragmented. Whereas deductive approach is used when “the structure of analysis is operationalized on the basis of previous knowledge and the purpose of the study is theory testing.” (Elo & Kyngäs, 2008:109).

In this dissertation, a deductive qualitative content analysis approach is adopted to analyse manufacturers’ manuals and reviewers’ documents from a security perspective. Both categories of the data are in electronic format. In the instance of electronic documents, although the data are

already captured, time is needed to prepare them for analysis. The reasons for this, according to Saunders (2011), is that,

- The data need to be appropriately anonymized by using separated codes for the researcher and the participants;
- The files should be stored appropriately to facilitate analysis;
- The files should be free of typography errors.

According to Vaismoradi *et al.* (2013:400), the purpose of content analysis is to “describe the characteristics of the document’s content by examining who says what, to whom, and with what effect”. One practical application of content analysis is to examine trends and patterns in documents (Stemler, 2001:2).

Elo and Kyngäs (2008:109) describe three main phases by which the process of content analysis should proceed, these include preparation, organization, and reporting as shown in Figure 2-3, on the next page. In the preparation phase, a researcher is required to transcribe an interview and obtain the meaning of the whole through reading the transcript repeatedly.

2.7.2.1 Preparation phase

According to Elo and Kyngäs (2008:109) during the preparation phase, a researcher needs to first decide what they want to analyse before selecting a unit of analysis. A unit of analysis can be a word, sentence, or a portion of the document. Once a unit of analysis has been selected, the researcher should ensure they make sense of the content. According to Vaismoradi *et al.* (2013:401), “every analysis requires a context within which the available texts are examined”.

The researcher must construct a world in which the texts make sense allowing them to answer research questions.” As soon as a researcher obtains the meaning of the content, he can then decide whether to develop categories or themes before he moves on to the next analysis step.

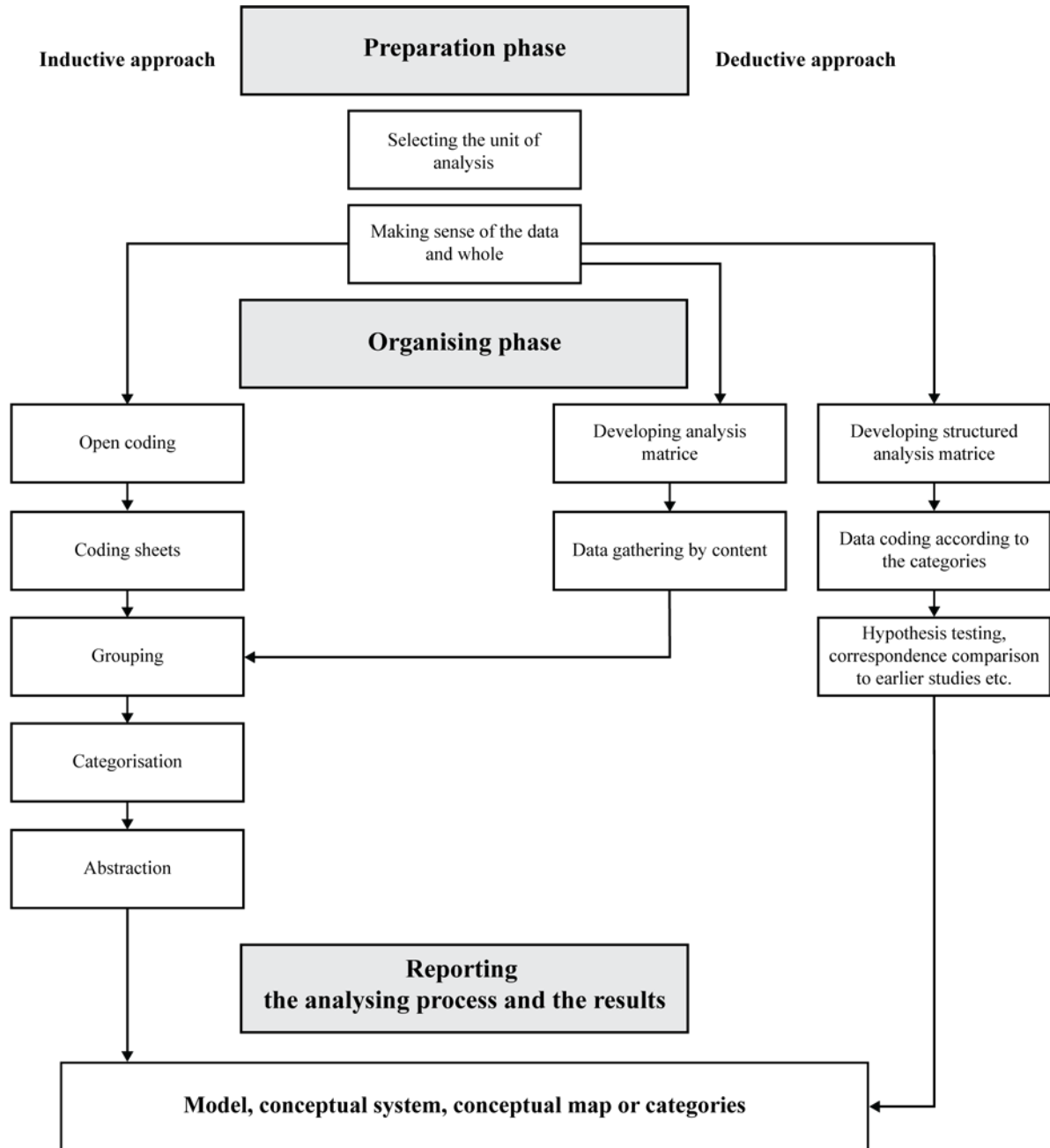


Figure 2-3 Content analysis steps (Elo & Kyngäs, 2008:110)

2.7.2.2 **Organizing phase**

Data that have been analysed using qualitative inductive content analysis approach, will need to be organized. For instance, a researcher might need to derive quantitative variables from qualitative data, this process is known as coding (Seaman, 1999:563). According to Thomas (2006), the purpose of coding include: “

- Condensing extensive and varied text data into a brief, summarized format;
- To establish clear links between the research objective and the summarized findings derived from the raw data;
- To develop a model or theory about the underlying structure of experiences or processes evident in the text data.”

When coding a document, one may consider what parts of the text need coding. Text to be coded can be divided into words, sentences, or a whole paragraph. These are known as coding units. Coding units fall under three categories, sampling, context, and recording coding units (Stemler, 2001:4). One needs to be careful though with the coding process and try to avoid losing the meaning or accuracy of the information during this process (Seaman, 1999:565).

2.7.2.3 **Reporting phase**

The last phase of the analysis process is the reporting phase. This phase’s aim is to present the results of the organizing phase. According to Vaismoradi *et al.* (2013:402), it is the researcher’s responsibility to be creative on how they present their findings, although presenting the results in a storyline, a map, or model is encouraged. Trochim and Donnelly (2001) discuss three important points that researchers need to keep in mind before they report on their findings. First, they have to think of the audience. Whom is this report aimed for? The report may look different based on the kind of the audience it is intended for. Is the audience looking for facts and details, or are they just interested in a summary of the findings? The second point to consider is the story of the research. Every research has a story to tell. A researcher needs to put him/herself in the shoes of the audience and try to understand what kind of story the audience will want to hear. The last point is what type of formatting the report will adopt. This last point is dependent on where the report will be published. The format will be different when the report is published in a book or a journal.

2.7.3 Interviews

According to Hyland (2016:116), interviews offer more interactive and less predetermined ways of eliciting information, compared to other methods such as surveys. Interviews can also help researchers to gather relevant data needed to answer research questions (Saunders, 2011:318). The flexibility of interviews results from the ability of the interviewer to ask auxiliary or follow up questions in order to get a better understanding of the interviewee. Interviews can be conducted face-to-face or can be done over the phone, or via a video chat. Questions used in an interview can be structured, semi-structured, or unstructured according to Wohlin and Aurum (2015:1441). Interviews are often used in qualitative technique for collecting data (Wohlin & Aurum, 2015:1441). In the following sections three types of interviews will be discussed, namely structured, semi-structured, and unstructured interviews.

2.7.3.1 *Structured interviews*

Structured interviews make use of a standard set of questionnaires administered by the interviewer (Saunders, 2011:320). The aim of a structured interview is to collect quantifiable data. The interviewer cannot add or change questions, and questions need to be asked in the order they appear on the questionnaires.

2.7.3.2 *Semi-structured interviews*

According to Tyson (1991:88), semi-structured interviews are intended to provide some flexibility during the interview. More information may be gathered from the interviewee, by asking auxiliary questions which may encourage the person to reveal more. One advantage of this method is that it is done face-to-face, and this may help the interviewee to say more than if the questions had to be answered on a paper. Saunders (2011:320) also states that questions ordering may not be followed when conducting a semi-structured interview. The interviewer may dictate the flow of the interview by selecting which questions to use.

2.7.3.3 *Unstructured interviews*

In unstructured interviews, the interviewer employs open-ended questions which allow the interviewee to be able to express themselves openly (Moyle, 2002:267). There is no list of structured questions according to Saunders (2011:321) Questions may take the form of, what do you think or tell us about yourself. Such questions will yield various answers from participant; hence no structured answers are expected. Answers may also be voice recorded and transcribed later. According to Corbin and Morse (2003:338), with unstructured interviews, the interviewer tries to create an intimate relationship with the interviewee allowing him/her to feel more comfortable. The results of such interviews are always unpredictable because the interviewee never knows what kind of secret may be disclosed.

Although there are no face-to-face interviews in this study, data collected from published, online reviews are considered as unstructured interviews. Therefore, the analysis of the documents will be similar to the analysis methods used in unstructured interviews.

2.7.4 **Grounded Theory**

Grounded theory is a both a data collection and data analysis method, rooted in symbolic interactionism (Heath & Cowley, 2004:142). Glaser (2017:1) defines grounded theory as a “*the discovery of theory from data – systematically obtained and analysed in social research*”. Wagner *et al.* (2010:7) describe grounded theory as a method for both collecting and analyzing data. According to Urquhart *et al.* (2010:361), grounded theory “*is independent of the underlying epistemology*”, meaning it has a neutral stance as a research method. They argue that this is because grounded theory has been used in positivist, interpretive studies, or critical social research studies. Thus, the ontological and epistemological position will depend on how the researcher applies grounded theory.

According to Saunders (2011:149), with grounded theory, data collection begins prior to the formulation of an initial theoretical framework. A researcher would have to generate theory from data which is created through observations. The collected data are again put through the process of predictions which are later tested to confirm these predictions. Grounded theory supports the epistemological perspective of interpretive methods in its approach to how theory is created in latter stages of the coding process.

Grounded theory has always been described as an inductive approach from its founding (Saunders, 2011:148). Heath and Cowley (2004:144) also discuss how induction has been the key to grounded theory, as researchers move from data to empirical generalization and on to theory as shown in

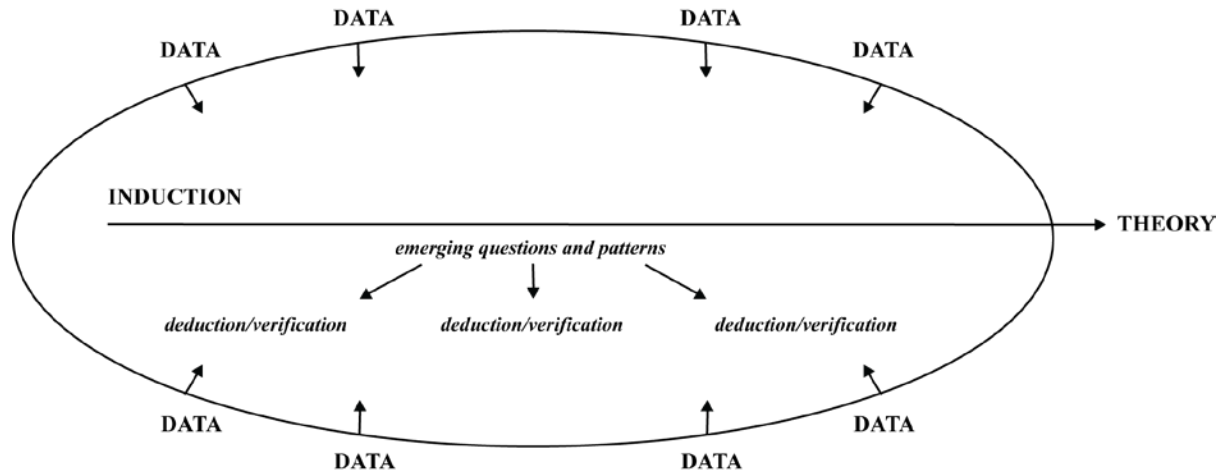


Figure 2-4 Induction, deduction, and verification in grounded theory (Heath & Cowley, 2004:144)

According to Urquhart *et al.* (2010:359) grounded theory has the following characteristics: “

- The main purpose of grounded theory is theory building.
- As a general rule, the researcher should make sure that their prior knowledge of the field does not lead them to the pre-formulated hypothesis that their research then seek to verify.
- Analysis and conceptualization are engendered through the core process of joint data collection and constant comparison, where every slice of data is compared with all existing concepts and constructs to see if it enriches any existing category, forms a new one or points to a new relation.
- Slices of data of all kind are selected by a process of theoretical sampling, where the researcher decides on analytical grounds where to sample from next.”

Grounded theory characteristics are applied in interpretive study as foundation for different data collection and analysis methods.

2.7.5 Document research

Document research is defined as a “systematic procedure for reviewing documents, both printed and electronic” (Bowen, 2009:27). Document research, like any other research method, involves

examination and interpretation of data in order to deduce meaning (Bowen, 2009:27). The word document may encompass many formats in addition to text-based documents, such as pictures, graphs, diagrams, field recordings, videos, and interview transcripts (Rapley & Jenkins, 2010:380). In this study, the word document solely refers to electronic-based documents, which include manuals, technical documents, white papers, and internet reviews.

Document research, although not used by many researchers as the main research method, qualifies well as a stand-alone research method, although in most instances it is used in combination with other qualitative research methods in a process known as triangulation (Bowen, 2009:28). As a qualitative research method, document research is mainly used with a qualitative case study, according to Bowen (2009:28).

2.7.6 Position of study

The source of the data used in the study, is from documents. Thus, document research in context of a case study, is used as the main method of data collection.

2.8 DETAILED RESEARCH PLAN OF THE STUDY

Figure 2-5 summarizes the selection of strategies and methods used in this study.

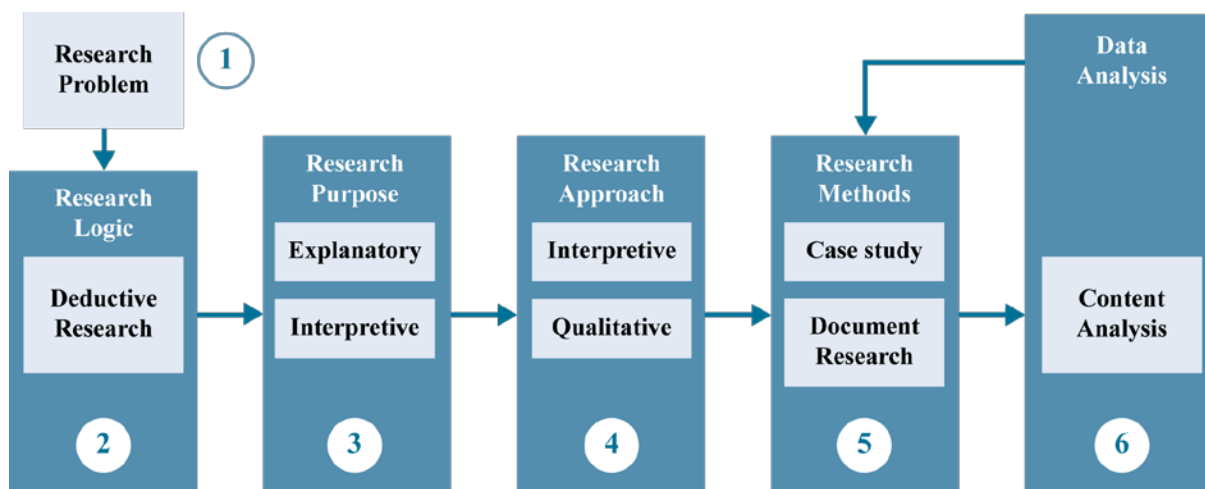


Figure 2-5 Research decision-making structure

The steps taken by this research, are adopted from a decision-making structure developed by Wohlin and Aurum (2015:1427). From figure 2.5, the first step of the research is to provide a well-defined research problem as discuss in Chapter 1, Section1.3.

In step two, a deductive research approach is adopted. As highlighted by Saunders (2011:92), with a deductive approach one uses literature to identify ideas and theories which can be tested using the data. This research logic is adopted since various forms of literature are be examined first, then only are data collected to enrich the understanding.

In step three, the purpose of this research is described. This researcher has adopted both explanatory and exploratory approaches. Saunders (2011:171) describes the purpose of explanatory research as the studying of a problem to establish the relationship between variables. In this research, that relationship is between the *introduction of smart objects in the home and their impact on data security*. The reason for using an exploratory approach has to do with the fact that the field of smart technology is still very new, with very little study done or information available, thus some exploration is vital. The only danger of exploring is that the research may change direction as a result of new data or insights (Saunders, 2011:171). In step four, two research approaches are adopted. After an extensive investigation into various research paradigms and research approaches, it was decided that this research falls well within the boundaries of an interpretive study, as well as the type of data that will be collected which is of qualitative nature. In step five, two research methods are adopted from the list of interpretive research methods discussed in Section 2.4. The research is case study-based, but it also combines document research as data collection method. In the final step (six), content analysis is selected as data analysis methods.

2.9 SUMMARY

The primary objective of this study is to identify the security threats which smart home devices may pose to unsuspecting homeowners concerning their data privacy. In this chapter a number of research approaches and methods are discussed in order to select an appropriate strategy for this study. Different research paradigms are discussed in Section 2.2, namely positivism, interpretivism, critical social theory, and DSR. From the contrast between these philosophies, an

interpretive stance is adopted for this study. This is because interpretivism attempts to explain reality from the viewpoint of the participants, which fits in well with the objective of this study.

In Section 2.4, a number of interpretive research approaches are considered. From these discussions, case study research is most suitable approach. Section 2.6 considers data collection methods used in qualitative research. This study focus is on the collection and analysis of data from electronic sources. The data come from two different sources, namely technical manuals and internet reviews. Thus, the only methods that qualify for this purpose are document research and unstructured interviews. An unstructured interview is selected because the same approach used here can also be applied to online reviewers' documents. These reviews are treated as transcribed interviews. This study is conducted deductively which implies that the empirical study aims to enhance the understanding formed by the theoretical investigation. Thus, the empirical study is not an independent method for theory development as is often the case in interpretive studies.

Content analysis is selected as data analysis method as discussed in Section 2.7.2. Content analysis is a laborious method because it requires investing a lot of time in the process to code the data, using similar coding strategies as open coding in grounded theory. The analysis process requires that the researcher makes sense of the text he is reading and use a method such as coding to summaries the information, in order to be able to present the findings in a way which makes sense.

In Chapter 3, the theoretical foundation of the IoT is presented including software, hardware, and networking aspects of IoT and smart devices.

CHAPTER 3 INTERNET OF THINGS

3.1 INTRODUCTION

In the early 1990s personal computers operated in isolation with no network connection capabilities. In the middle of the 90s though, personal computers were sold with networking capabilities allowing them to be part of a network. In the middle of the 2000s, with the introduction of smartphones, home areas networks (HAN) comprised of devices other than just computers. Today a HAN has evolved again, television sets, home appliances such as fridges and washing machines are now capable of connecting to a HAN and communicate with other devices. This interconnection will be referred to as a connected home, or a smart home.

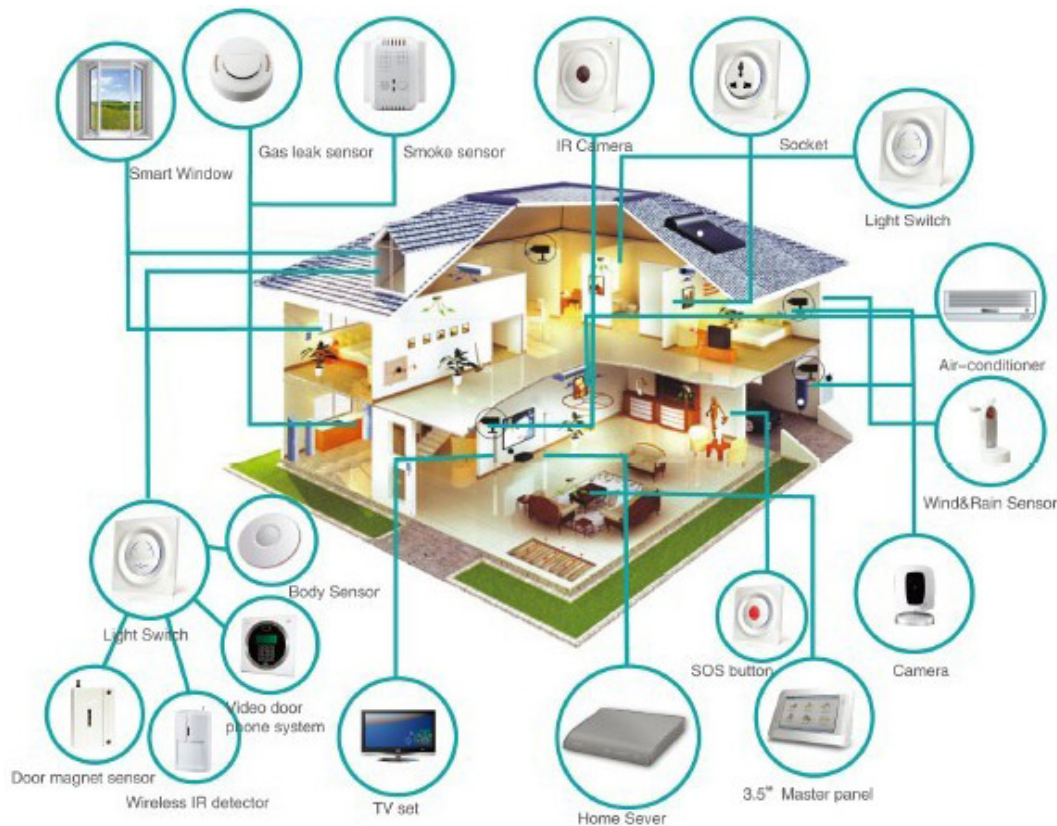


Figure 3-1 A representation of a smart home (Smarthomeenergy.co.uk, 2019)¹

¹ Permission to use artwork was requested.

Many definitions exist when it comes to describing what a smart home is, such as Smarthomeenergy.co.uk (2019): “*a home that incorporates advanced automation systems to provide the inhabitants with sophisticated monitoring and control over the building’s functions.*” IoT is expected to be a revolution in the way common devices will be able to connect to the internet (Lamaazi *et al.*, 2014:328). IoT technology is made possible by various features such sensors (Mois *et al.*, 2017:2056); availability of embedded operating systems, such as Contiki, TinyOS, FreeRTOS and many more (Javed *et al.*, 2018:2062; Musaddiq *et al.*, 2018:8459); and network protocols that have been designed with power efficiency in mind (Al-Sarawi *et al.*, 2017:685).

IoT technology has changed the dream of a smart home into a reality. The availability of micro sensors, embedded platforms, and open-source operating system, such as Linux, have made it possible to build intelligence into everyday objects making them smart (Polianytsia *et al.*, 2016:152). Sensors have been used in various applications of IoT (Mois *et al.*, 2017:2056). For environmental usages, sensor-enabled devices can now be deployed around a home to read various data, such a humidity, water leakage, or carbon monoxide in case of fire detection. The difference between a common appliance/device and a smart one is the ability of the smart object to collect data about its environment (Hernandez *et al.*, 2014:2) and be able to communicate that data to another device which can take action. This ability of one connected object being able to communicate with another and take action without any interference from a human, is referred to as machine-to-machine communication (M2M) (Esfahani *et al.*, 2019:288).

For the common homeowner, all this technology may be overwhelming, even more so when security is a major issue in IoT networks (Khan & Salah, 2018:395). The aim of this chapter is to describe in detail the ins and outs of IoT, communication mechanism, protocol conventions, and other technical details that will make IoT operable. The term “smart home” will be used to describe a house that comprises of various types of appliances, devices, and sensors which will enable certain functionalities in the home and around the home to be intelligently automated.

From what has been described in the few paragraphs above, it is clear that the realization of the IoT relies on six major aspects, the smart appliances and devices themselves (Section 3.2), smart electricity management (Section 3.3), sensors (Section 3.4), the central controlling device, called the IoT hub or gateway (Section 3.5), the operating systems used by the devices (Section 3.6) and finally networking aspects (Section 3.7). The availability of these underlying technologies and

their integration has made IoT a reality today. From a security perspective the position of the researcher is that each component of the smart home has its own vulnerabilities. In the following sections, we will look at these various technologies, and how each plays a role to enable understanding of the complete smart home from a security perspective.

3.2 SMART APPLIANCES AND DEVICES

A HAN in smart home comprises of many devices which are interconnected and able to communicate. These include smart devices (e.g. TVs and speakers.); smart appliances (e.g. fridges, dishwashers, etc.); smart things (e.g. smart locks and smart thermostats); smart grid (e.g. smart meters) and the smart hub or IoT gateway which is at the heart of each smart home. Smart appliances such as fridges, cookers, washing machines, vacuum cleaners, dishwashers, just to name a few, are said to make lives easier in a home (Grogan, 2012:44). What makes these appliances smart? The word smart in “smart appliances” can mean two things, one is that the smartness has to do with the ability of these devices of being able to communicate with other smart devices such as a cell phone or tablet, allowing a homeowner to be able to control the smart appliance remotely (Grogan, 2012:44). The other reason is the ability of these devices of being able to connect to the grid and the internet.

3.2.1 Selection of smart appliances and devices investigated in this study

Smart appliances come in different forms and shapes, and every household appliance’s manufacturer today seem to be creating a smart version of the appliances they manufacture. The aim of this study is to identify threats to users posed by incorporating these devices in their homes. Security threats are the result of specific functionalities of these devices which in turn result from specific components and sensors used in the device along with its connectivity. Connectivity in terms of a local network and in terms of the internet. In a study such as this one, the researcher has to select items to study which is representative of similar items not studied. From the vast diversity of smart devices, a selection is made for further investigation, this selection is based on two aspects (1) on their availability and adoption in South African homes, in order to have reviews available and (2) the components, especially sensors used by the devices to gather data. The devices selected are: smart televisions, speakers, locks, fridges, washing machines and cameras. Gateways are also

part of this study as discussed in Section 3.5. Motivation for the selection of these appliances and devices are provided as part of the discussion.

3.2.1.1 *Smart televisions*

A smart television is defined as a “*type of TV with set-top box or with internet facilities allowing ability of computing and advanced type of connectivity*” (Reuters, 2018). The main advanced features may include installation of applications, built-in cameras for motion controls, built-in microphone for voice control, Wi-Fi connectivity and internet capabilities. (Samsung, 2018).

The adoption of smart TVs has been tremendous in the past years, which is reflected by the market value. By 2018 the global market for smart TVs was reported to be around 157 billion US dollars (Wold, 2019) with the market leader being Samsung (Reuters, 2018). It is clear from this data that smart TVs are the most popular smart appliances found in many households today. Hence the security of these appliances should be of great concern.

For instance, the Samsung UN65NU800DFXZA smart TV, comes with features such as a microphone, connectivity via Wi-Fi or LAN, and an operating system. Most of these smart TVs come with software libraries that are known to have vulnerabilities making them susceptible to attacks (Michele & Karpow, 2014:351) Samsung’s privacy policy page (Samsung, 2015) acknowledges that they do collect data from these devices. This data is transmitted over the internet making it subject to man-in-the-middle attacks.

Suppliers of smart TVs fall under two categories:

- I. *Platform-based*: This category comprises devices such as Google and Apple TVs. These smart TVs are provided as a set-top box, with the ability to connect to the internet and able to stream movies and TV shows. Apple TV is only one made by the company itself, whereas android TV is provided to many hardware manufacturers who are able to implement it in their own set-top boxes.
- II. *Digital appliance-based*: This category comprises of TVs from manufacturers such as Samsung Electronics and LG. These manufacturers do have their own operating systems that they have implemented on their TV sets, but with the collaboration with Google, many of the TVs also come with Android as an operating system.

Security aspects of smart TVs are investigated empirically since they use two common sensors, cameras and microphones, to collect data. They can be controlled remotely and have scheduling ability. TV's has the functionality to be connected to the local network and internet which opens the potential for many threats based on these vulnerabilities. Different TV's brands use different operating systems, with specific vulnerabilities. These characteristics are used in Chapter 6 to list the vulnerabilities of smart TV's from a literature perspective.

3.2.1.2 *Smart speakers*

Smart speakers are wireless voice-controlled speakers, with the ability to understand voice commands and the ability to execute certain functionalities (Lenovo, 2019). For instance, with popular smart speakers such as Google Home (Google, 2019b), amazon's Echo dot (Amazon, 2019c), or apple's Homepod (Apple, 2019), users can use the various voice assistants that come with the speakers to execute simple tasks such as playing music or setting up an alarm, to more advanced tasks such as calling a taxi or placing an order online. All these speakers come equipped with an operating system, Wi-Fi connectivity, and very powerful microphones. The convenience such devices bring to a smart home cannot be undermined, but in addition to that, these speakers can be a real security risk to homeowners (Lau *et al.*, 2018).

Although not all speakers are equipped with cameras, the always-on microphone and connectivity of smart speakers, lead to similar security vulnerabilities as in the case of Smart TV's. A specific characteristic of a smart speaker that is more problematic in the speaker as in the TV, is the fact that it becomes part of the household, the unsuspecting homeowner names it, and treats it as a "human" without realising that it may collect, store and transmit data on a continuous basis.

3.2.1.3 *Smart locks*

Midrack (2019) describes a smart lock as a Wi-Fi or Bluetooth-enabled smart device that permits being controlled remotely via a mobile device by sending secure signals to lock or unlock. The market for such devices is growing and many companies provide a variety of smart locks to choose from as indicated in Table 3-1.

Table 3-1 Comparison of smart locks adapted from Delaney (2019)

	Yale Assure Lock SL (YRD 256) with ZigBee	August Smart Lock Pro + Connect	Schlage Sense
Reference	Yale (2019)	August (2019b)	Schlage (2019)
Connectivity	ZigBee	Bluetooth/Wi-Fi/Z- Wave	Bluetooth
Integration	Amazon Alexa, Apple HomeKit	Amazon Alexa, Apple HomeKit, IFTTT	Amazon Alexa, Apple HomeKit, Google Assistant
Application	Mobile	Mobile	Mobile
Geofencing/locations services	X	✓	X
Guest access	✓	✓	✓
Tamper alarm	✓	X	✓
Touchpad	✓	X	✓
Voice activation	✓	✓	✓
Battery operated	✓	✓	✓

Table 3-1 provides a brief summary of popular smart locks on the market. As can be seen from this list, a smart lock can incorporate a number of features. For instance, a user can be able to lock, unlock, and monitor doors remotely from anywhere using a mobile device. Logs of all the access can be saved, allowing you to know who entered your home. The geofencing feature allows a user to open the door automatically once the lock is able to detect the phone nearby. The locks have abilities to also automatically lock after a specified amount of time. The integration with smart speakers allows homeowners to active these locks using voice commands. For instance, with the Yale smart lock, a user can generate digital keys and share them, maybe with guests. This feature allows your guest to access your home even if you are not around.

Just as it is with any other smart home device, smart locks still pose the danger of their being compromised by an intruder. The remote control functionality of the lock and the high risk of loss when an attack occurs motivate the inclusion of these devices in the empirical study.

3.2.1.4 *Smart fridges*

The idea of a smart fridge might sound like a gimmick to some. Many people would ask themselves why one would need a smart fridge. A fridge is classified as being smart based on its ability to connect to the internet and allowing communication with the homeowner. For instance, a smart fridge can be able to give us advice on what we should eat, when we should eat, and how it should be prepared (Grogan, 2012:45). The market for a smart fridge is growing due to the quick adoption of the technology. The LG InstaView (LG, 2019c) smart fridge comes with a list of smart features, among them is the mirror door that can turn clear by knocking on it, allowing the owner to view inside the fridge without opening it. Another smart technology is what LG calls SmartThinQ (LG, 2019d). This technology allows the owner to remotely connect by his phone to the fridge and being able to perform functions such as checking the expiring dates of products or checking the inventory of products in the fridge. Other smart features included in the LG smart fridge are smart grid; smart diagnosis, smart manager, and smart chat (LG, 2019c):

- *Smart grid* function allows the fridge to communicate with a utility company when the fridge is connected to the internet via Wi-Fi.
- *Smart diagnosis* allows the mobile app to collect data from the fridge and send this data to a technician for troubleshooting purposes. Minor faults are sent as alerts to the owner's phone app, and serious errors are sent to an LG service centre helping them to determine if a technician should be dispatched (Grogan, 2012:46).
- *Smart manager* allows interaction between the smart fridge and the owner via a mobile app. The owner is enabled to get information about the content of the fridge.
- *Smart chat* is an additional feature, which makes use of the Line chat application allowing the owner to communicate with the fridge using text messages.

These features enhance the functionality of the fridge by making it smarter than an ordinary fridge, yet these features open a door to all kinds of network security risks by allowing the fridge to be remotely controlled over the internet. As evident from the list of functionalities provided, a smart

fridge contains many technologies present in smart devices which makes it crucial to include in the empirical investigation.

3.2.1.5 *Smart washing machines*

Smart washing machines come with built-in Wi-Fi connectivity features, remote management, and internet capabilities. For instance, the LG WM9000HVA is a smart Wi-Fi enabled washer. With the support of the SmartThinQ app, a homeowner can remotely control the washer. While the washer is busy, the owner can be notified of the progress of the job via the mobile app. The owner also gets notifications about scheduled maintenance of the machine. The smart diagnosis feature allows the machine to report errors to the manufacturers on its own. With the popularity of smart speakers, LG has incorporated the ability for the user to control the washer using voice command via Alexa or google home.

The security threats of smart washing machines are comparable to those of smart fridges and is therefore not included in the empirical study. However, their control by means of a mobile app and a smart speaker are important characteristics investigated in the empirical study. Various other devices have the functionality to be connected to a home control unit or gateway, to be controlled by means remote mobile phone app or even smart speaker. Home control units or gateways are investigated empirically in this study.

3.2.1.6 *Smart cameras*

Surveillance cameras play a huge role in the security of a home, it can be used to monitor what is happening inside your home, as a baby monitor, or to see who is at the door. Unlike traditional cameras which could only be used to just take photos or video for surveillance, smart cameras now have some degree of intelligence built into them, such as pattern recognition and image processing. This allows them to read number plates of cars, or be able to recognise someone's face (Shi & Lichman, 2005:1). A number of smart cameras for home use are available for purchase today. Table 3-2 lists a selected number of smart monitoring cameras and the features each provides in comparison to its competitor. The majority of these cameras don't have a local storage facility, rather they save everything in the cloud. This creates a security risk whereby videos of your children end up being uploaded to the cloud. These cameras may be convenient for people who want to monitor their homes while at home or on holiday. Since they support internet connectivity,

a user can connect to the camera using their mobile device from anywhere. More on the features and benefit of these cameras, refer to their manuals. Security is always a challenge these days for any interconnected device. Having smart cameras in our homes recording us all the time has its own benefits, but in the wrong hands it can become a serious privacy infringement when an unauthorised user is able to take control of these cameras.

Table 3-2 Comparison of smart cameras features, adapted from Wollerton (2019)

	Arlo Pro 2	Canary Flex	Logi Circle 2 (Wired model)
Reference to source	Arlo.com (2019)	canary.is (2019)	Logitech (2019)
Type	Indoor/outdoor	Indoor/outdoor	Indoor/outdoor
Power source	Rechargeable battery/power adapter	Rechargeable battery/power adapter	Power adapter
Resolution	1080p HD	1080p HD	1080p HD
Battery life	6 months	2 months	N/A
Live stream support	✓	✗	✓
Cloud storage support	✓	✓	✓
Local storage support	✗	✗	✗
Mobile app	✓	✓	✓
Night vision	✓	✓	✓
Activity zones	✓	✓	✓
Alerts	Motion and audio	Motion and person	Motion
Third-party integration	Amazon Alexa, Apple TV, Google Assistant, IFTTT	Amazon Alexa, Apple TV, Google Assistant, Wink	Amazon Alexa, Apple HomeKit, Google Assistant

In this study cameras are viewed as sensors with specific vulnerabilities, leading to vulnerabilities in all devices that use them. These vulnerabilities are also present when they are used as independent devices. Cameras are not separately investigated in the empirical study but due to their integration in other devices, much investigation is presented on vulnerabilities and resulting threats based on the inclusion of a camera in a specific device.

3.2.2 Benefits of smart appliances in a household

Smart appliances are said to bring convenience to a homeowner, making life much easier than with traditional appliances. What is however of great benefit is the ability of these appliances conserve energy.

- I. *Convenience*: The value of a smart appliance is not limited only to what the appliance can do, but more so to the services, the appliance can provide through the cloud (Uehara, 2015:457). Smart appliances are said to enhance the livelihood of a household by making life easier. For instance, the homeowner can remotely query the status of a washing machine to see if it is done with the washing, or the homeowner can be able to check remotely what is missing in the fridge if they forgot to check the fridge before leaving home.
- II. *Energy saving*: A study conducted by CSIR in 2010 (Rasuba *et al.*, 2010:6) illustrates how the demand for electricity consumption has increased over the decades in a normal South African's household. Stragier *et al.* (2010:137) believe that increased demand for electrical appliances in many households today is of great concern for the energy requirements or demand for each household. This may also be true of many households in South Africa. According to Stragier *et al.* (2010:136), inefficient use of these appliances can result in great wastage of energy. Changing the pattern of electricity consumption in a household is crucial in addressing energy wastage. Many smart appliances have the ability to generate data that could be used to learn of the energy usage of the device. This data can then be used by analytical software to advise the homeowner of his energy consumption behaviour and ways in which he can save energy (Dirienzo *et al.*, 2014:188).

It was shown that vulnerabilities of smart devices result from specific characteristics. The remainder of the chapter presents technical information in support of the identification of vulnerabilities based on specific components.

3.3 SMART ELECTRICITY MANAGEMENT

No smart appliances or other smart devices in a HAN can operate without electricity. To make a house in a HAN really smart, the electrical side of the house should be made smart as well, through the use of smart electricity meters and smart electricity grids.

3.3.1 Smart electricity grid

The advancement in technology has made it possible to develop an intelligent energy management system to accommodate the ever-growing energy demand. This intelligent energy management system is what is referred to as a smart grid (Bitzer & Gebretsadik, 2013). A smart grid can be characterized by the dual flow of both electricity and information which makes it possible to create an automated, distributed energy delivery network (Panajotovic *et al.*, 2011:118). In a smart grid, smart electricity meters and sensors are used to collect data from the end user's appliances, an enormous amount of data can be collected and stored in the cloud (Panajotovic *et al.*, 2011:1). Many of the smart appliances we have discussed so far come with the ability to connect to the smart grid. The benefit of this functionality is discussed in Section 3.2.2. More research has been conducted on smart grid technology and its security risks as described in Table 3-3.

Since HAN users do not have control over their involvement in smart grids, the topic is not explored in more detail in this study. The homeowners should however be aware of the consequences of smart meters as discussed in the next section.

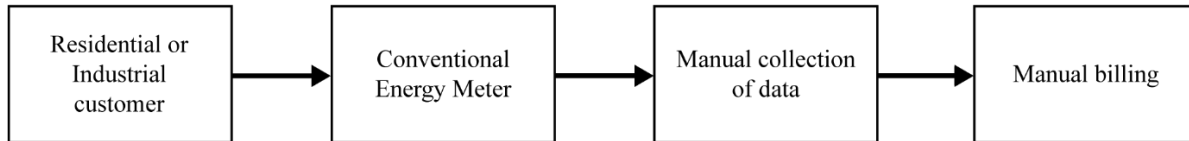
3.3.2 Smart meters

In many parts of the world traditional electricity meters are still being used to read the energy consumed by the client. Recently though, electronic meters were introduced with the capabilities of reading energy consumption remotely (Dede *et al.*, 2015:1). The smart meter plays a key role in the interaction of the client and the utility supplier (Khan *et al.*, 2014:75). Figure 2-1 shows a comparison between a traditional meter and a smart one. The major differences are found in the methods used for collecting usage data, the billing method, and the storage of the collected data.

Table 3-3 List of researches conducted on smart grid technology and its security.

References	Research topic	Focus area	Summary
Yong <i>et al.</i> (2011)	Analysis of Smart Grid security standards	Security in smart grids.	The research investigates vulnerabilities which exist in smart grid technology that may expose the network to cyber-attacks.
Farag <i>et al.</i> (2014)	Cross-layer security framework for smart grid: Physical security layer	Security of process control systems in smart grids.	The research considers the impact of cyber-attacks on the physical domain of smart grids and proposes a cross platform security framework that can help in preventing attacks on both the cyber and the physical side.
Rawat and Bajracharya (2015)	Cyber security for smart grid systems: Status, challenges and perspectives	Current status of the technology and the challenges it poses.	The research provides an overview on the current state of the technology and what type of challenges the technology faces, especially when it comes to keeping smart grids secure.
Erol-Kantarci and Mouftah (2015)	Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues	Communication infrastructure of smart grids.	The research is a survey on the smart grid-driven approaches in energy efficient communications and data centres, and the interaction between smart grid and information and communication infrastructures.

Conventional Energy Meter



Smart Meter System

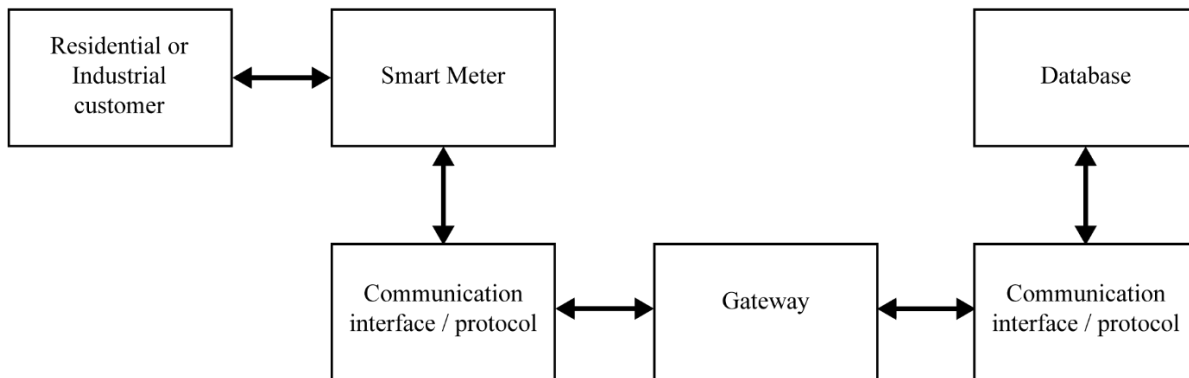


Figure 3-2 Comparison of a traditional electricity meter and a smart meter architecture (Depuru *et al.*, 2011:2737).

The implementation of smart meters results in a massive amount of data flowing between the utility and company and the smart meter itself (Depuru *et al.*, 2011:2739). This data is transmitted remotely to a utility company over the internet. Some of the protocols such as DNP3, implemented for communication to smart meters, are known to have security concerns (Depuru *et al.*, 2011:2739). Connecting the smart meter to the internet can open up the system to a number of vulnerabilities and attacks such as unauthorized data access, an attacker turning off all devices remotely, smart metering data repudiation, stealing electricity without being noticed, and causing an outage by attacking the smart grid physical infrastructure etc. (Gao *et al.*, 2012:400). Homeowners do not have control over the functionality of smart meters in the South African where this study is performed. Smart meters were excluded from the empirical investigation.

3.4 SENSORS AND SENSOR NODES

Sensors are electronic circuits that are able to sense a change of energy from one form to another. The energy can be in the form of movement, electric signals, radiant energy, thermal energy, magnetic energy etc. Sensors come in both digital and analogue form. In a nutshell, a sensor can be described as a device that acquires information from a real-world (Mason, 2015:2). Sensors are normally used for input purposes since they can be able to sense the change in the physical world as listed in Table 3-4 on the next page.

In a smart home, sensors may be placed in strategic areas or attached to certain appliances. However, sensors can't be deployed on their own, they need to be part of a system. These are normally referred to as sensor nodes. Sensor nodes hardware come in three formats, augmented general-purpose personal computers, dedicated sensor nodes, and system-on-chip sensor nodes (SoC) (Zheng & Jamalipour, 2009:11).

3.4.1 General-purpose PCs

This category of sensor nodes include low-power embedded PCs and Portable Digital Assistants (PDAs), which are mostly running on operating systems such as windows mobile, android, Linux, or real operating systems (Zheng & Jamalipour, 2009:11). This category of devices normally makes use of common network communication protocols such as Wi-Fi and Bluetooth. The

processing capabilities of this category is also much better compared to the other two categories discussed later.

Table 3-4 List of common sensors and transducers (ElectronicsTutorials, 2015)

	Input Device (Sensors)	Output Device (Actuator)
Light level	Light Dependent Resistor (LRD) Photodiode; Phototransistor Solar cell	Lights & Lamps LED's Displays Fibre optics
Temperature	Thermocouples Thermistor Thermostat Resistive Temperature Detectors	Heater Fan
Position	Potentiometer Encoders Reflective/Slotted Opto-switch LVDT	Motor Solenoid Panel meters
Force/Pressure	Strain gauge Pressure switch Load cells	Lift & Jacks Electromagnet Vibration
Speed	Reflective/Slotted Opto-switch Doppler Effect Sensors	AC and DC motors Stepper motors Brake
Sound	Carbon microphone Piezo-electric crystal	Bell Buzzer Loudspeaker

3.4.2 Dedicated sensor nodes:

This category of sensor nodes is characterized by small factor nodes, with low power consumption and communication, and making use of off-the-shelf chips (Zheng & Jamalipour, 2009:11). An example of these is the Medusa MK-2 node.

3.4.3 SoC nodes

According to Zheng and Jamalipour (2009:11), this category of nodes aims at extremely low power consumption and very small design footprint which will combine sensing, computation and communication capabilities. To achieve this small design footprint, the manufacturing technology used for these types of nodes is known as Microelectromechanical systems (MEMS). Zheng and Jamalipour (2009:9) describe MEMS technology as key to manufacturing tiny, low-cost, and low-power sensor nodes, where micromachining techniques are used to manufacture micron-scale mechanical components. A good example of this category of sensor nodes is Smart Dust (Frost

Gorder, 2003:6-9). An extremely small node running on Tiny OS (Alagupandi et al., 2014:104). Smart Dust is designed to occupy a volume of 1mm^3 , which is a typical size for a dust particle. They contain sensors, communication circuitry, and memory under 1 kilobyte (Sharifi et al., 2009:258). They are deployed in a wireless sensor node (WSN) depending on the sensors it possesses.

3.4.4 Design characteristics of the sensor node

To design sensor nodes which meet the requirements of their tasks, a few design factors should be taken into consideration. These factors also have a serious impact when it comes to the design of WNS (Zheng & Jamalipour, 2009:6). These design factors include:

- I. *Size*: Sensor nodes are normally deployed in environments where they should be invisible (Savvides & Srivastava, 2002:2), thus a small size will be very important. The small size also helps with deployment, at the time these sensor nodes might be deployed in harsh environments in large quantity (Zheng & Jamalipour, 2009:6);
- II. *Cost*: Sensor nodes are designed with a view to being disposable and deployed in large quantity (Savvides & Srivastava, 2002:2), hence producing them at a cheaper cost is very important;
- III. *Power efficiency*: Since these nodes are designed with one-use in mind, they need to be powered long enough for them to be of any good use. Zheng and Jamalipour (2009:6) argue that this is the most important design factor since these nodes are powered by batteries which cannot be changed or recharged;
- IV. *Flexibility*: Sensor nodes should be able to support a number of additional hardware sensor interfaces and also be very flexible when it comes to the programmability (Savvides & Srivastava, 2002:2);
- V. *Security*: When it comes to the security aspect of the design, Zheng and Jamalipour (2009:7) focus only on the military side of application. Although this is very important, based on where these sensor nodes are deployed, security should always be a concern.

In this dissertation the focus of sensor nodes deployment is limited to a smart home. Even in this setup, security should be our number one priority if we want to protect these nodes from unauthorized access. Sensors are a major part of an IoT network.

3.4.5 Radio Frequency Identification

A radio frequency identification (RFID) system is described by Jia *et al.* (2012:1282) as “an automatic technology and aids machines or computers to identify objects, record metadata or control individual target through radio waves”.

The term IoT also refers to the ability of identifying objects in a network. RFID plays a vital role in this aspect (Jia *et al.*, 2012:1282). For instance Hussain *et al.* (2009:150-157) describe the application of RFID in smart homes, where RFID tags can be used in conjunction with WSN to identify motion within an environment and also be able to track objects within a home. For example, a tagged person can be identified when they go in and out of a door, or objects in a home such as keys and remotes can be tracked if misplaced.

Hu *et al.* (2009) describe a system that can be used in a hospital to dispense prescriptions to patients. This wearable medication platform hosts an RFID reader which is capable of RF communication with patients. The patient scans his/her medication bottle, equipped with an RFID tag, and the scanned information is then wirelessly transmitted to a central computer for processing. If it happens that the patient is incorrectly taking the drug, he will be warned by a red LED toggle on their wearable device. In addition, the healthcare employee managing the workstation will also receive a message signalling that a patient has tried to improperly take a drug.

Figure 3-3 shows the structure of an RFID system. It comprises of a tag (transmitter/responder), a reader (transmitter/receiver), and an application. Communication is initiated from the application, as a command, which is then received by the reader and forwarded to the tag. The response from the tag goes through the same steps in reverse. The tag itself is a small microchip with an antenna (Jia *et al.*, 2012:1282).

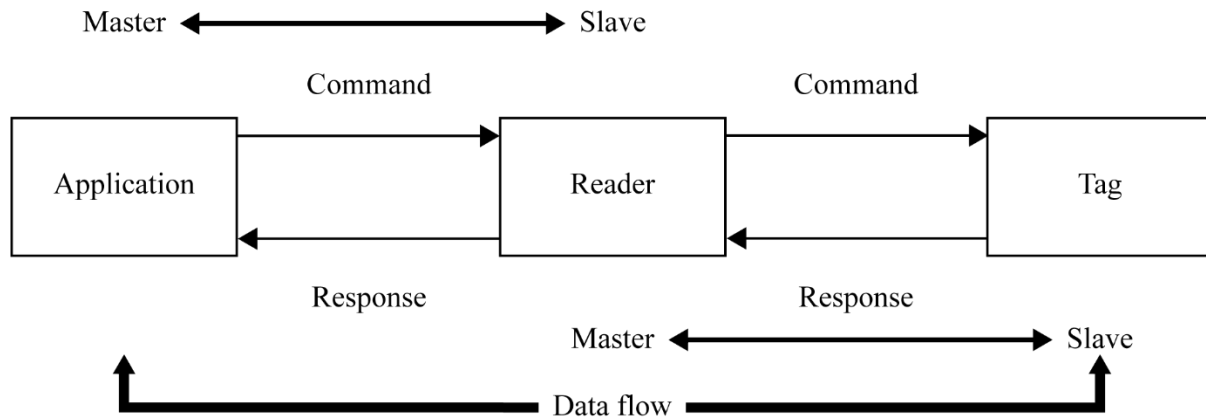


Figure 3-3 Components of an RFID system (Jia *et al.*, 2012:1283).

3.4.6 Actuators

Actuators are mainly used to control an external device, we can refer to it as any device that is able to generate a signal that can control a device (Mason, 2015:2). An example of a sensor and an actuator working together would be in an irrigation system. Humidity sensors may be placed in the soil, and as soon as the humidity becomes low, signalling lack of water in the soil, the sprinkler system will be switched on to start the irrigation process. Once the humidity has reached the optimal level, a signal will be sent again to the sprinkler system to switch off. In this scenario, an actuator will be connected to the sprinkler system to switch it on and off.

Apart from scenario described above, sensors have found applications in any aspect of our lives, they have been used in health care (Dhar *et al.*, 2014:152), environmental monitoring (Abbasi & Younis, 2007:2826), military application such as remote sensing (Zhang & Zhu, 2011:507), industrial process control, security and surveillance (Zheng & Jamalipour, 2009:5), and more recently in home intelligence such as smart homes (Hussain *et al.*, 2009:153; Lu *et al.*, 2010:211-224).

The majority of sensors used in IoT are digital wireless sensors. These sensors can be attached to inanimate objects such as, a carton of milk, a car, machines etc. as well as to animate objects such as animals, for the purpose of monitoring, tracking, and interacting with such objects (Haller, 2010:1). This interaction and monitoring require that these sensors be connected to a network. The network made with sensor nodes is referred to as Wireless Sensor Network (WSN) (Zheng & Jamalipour, 2009:12), more details on WSN are covered in Section 3.7.

In a smart home, sensors such as a humidity sensor can be used to monitor water leakage on a pipe or geyser, gas and temperature monitoring such as with the Nest thermostat.

3.4.7 An example: Nest thermostat

The Nest thermostat is a smart thermostat that comes enabled with Wi-Fi or ZigBee, and with a variety of sensors, from carbon monoxide sensors to temperatures sensors, allowing it to connect to the Nest Cloud, allowing one to remotely control it. (Hernandez *et al.*, 2014:2). The research conducted by Hernandez *et al.* (2014:2) also found out that the thermostat prompts users about their place of work and residence addresses. This information is believed to be shared with the utility providers. This information, together with the usage statistics are uploaded to the Nest Cloud via the internet. The fact that this thermostat is able to learn from the homeowner's usage behaviour and able to transmit such data to cloud-based servers, makes the thermostat a possible target for attackers.

Various devices and appliances are said to be smart due to the fact that sensors have been incorporated into these devices. Thus, the design characteristics of sensors are of great importance to the design of a secure IoT network. The position of the researcher is that the presence of sensors leads to specific vulnerabilities in devices. The operating systems used in the devices and their connection to gateways and the internet further increases the vulnerabilities of these devices.

3.5 IOT GATEWAY

The IoT gateway (also known as a smart hub), is a central interconnecting device in a HAN. Due to the lack of a common communication standard (Zhu *et al.*, 2010:347), many IoT devices use protocols other devices might not be using. This problem hinders the M2M communication that characterizes IoT (Datta *et al.*, 2014:514). In addition to this, many objects that have sensors on them may not be using internet protocol (IP) address for communication. These devices might be using protocol such as ZigBee, Z-wave, and 6LoWPAN which are designed for devices which consume less power (Lu *et al.*, 2011:267). To be able to bridge an IP based network, such as Wi-Fi and a WSN, an IoT gateway plays an important role of making sure these different technologies can still be able to interact with one another (Zhu *et al.*, 2010:347). One way the gateway is able to do this, is through its ability to support various types thereof. The IoT gateway is able to operate

as a protocol translator, encapsulating data from one protocol to another, allowing a smooth communication to take place (Shang *et al.*, 2013:722). The need for protocol translation, is due to the fact that WSN uses protocols that are not compliant with TCP/IP protocols used by most traditional networks (Emara *et al.*, 2009:1775), and also due to the fact that WSN protocol cannot directly communicate on the internet (Datta *et al.*, 2014:514). Another important role the IoT gateway plays, is to provide interconnection to all the connected devices in a smart home, creating a HAN in the process. This network is vital because it allows sharing of resources among the connected objects. A third role played by the IoT gateway is that of connecting a HAN to the internet. The connection is achieved through either DSL or 3G/4G connection. This connection makes it possible for most of the devices, appliances, and even sensor nodes to connect to the internet for remote management.

An IoT gateway is already described as a bridge which connects traditional networks (DSL, Wi-Fi, 3G/4G etc.) and sensor networks (Shang *et al.*, 2013:720). The functionality of an IoT gateway can better be understood by dissecting its structure. An IoT gateway architecture is divided into three layers, the perception layer, the transmission layer, and the application layer

- I. *Perception layer:* A WSN consists of sensor nodes equipped with either sensors or RFID tags. The perception layer job is to make use of these sensor nodes to collect data about the surrounding physical world. The data collected is then transmitted to the next layer using one of the communications available, such Bluetooth, RFID etc. (Zhu *et al.*, 2010:348).
- II. *Transmission/Network layer:* The data collected by WSN nodes in the perception layer is received by the network layer which then acts as a middleware between the perception and application layer (Zhang & Zhu, 2011:509). The transmission layer also has the job of transmitting the collected data to application servers over long distances using wired or wireless communication technologies such as DSL or 3G/4G/LTE (Zhu *et al.*, 2010:349).
- III. *Application layer:* Due to the limitations in hardware processing capabilities, most IoT based devices rely on servers, mainly found in the cloud, for processing the data collected from the perception layer. The main role of the application layer is to provide an information service. It comprises of the IoT client-side, data storage, and data inquiry modules (Zhang & Zhu, 2011:509). The application layer plays a twofold role, first it

presents the data to the services running on the servers for computation and analysis, and it secondly also provides the result to the users (Zhu *et al.*, 2010:349).

The three layer architecture can be refined into a four layer architecture presented by Vijayalakshmi and Arockiam (2016:34) which is commonly used for IoT environments by dividing the application layer into a support layer for cloud computing and an application layer for the user application. This four-layer architecture is used in this dissertation to guide the investigation on security matters in a HAN.

3.5.1 Security concerns of IoT gateways

Each of these layers leads to specific security vulnerabilities when gateways are used in smart homes. The perception layer has inherent all the vulnerabilities of the all the sensors connected to it. Temperature and light sensors may be manipulated by attackers to achieve a desired breach in security. The network layer, if not sufficiently protected is vulnerable to network attacks. Network connectivity is present in the form of various formats as listed above and each of these formats creates different vulnerabilities. The application layer is responsible for a vast amount of vulnerabilities in terms of data storage in the cloud or on the device but also in terms of the mobile device software used to control the functionality of the gateway. The hardware capabilities in terms of memory and processor along with the operating systems also have an impact on the gateway to create a secure smart home. The empirical investigation presented in Chapter 5 investigates the functionality of gateways in terms of the architecture presented here. The ability provided to the user to control security settings is an important consideration when selecting a gateway for a HAN.

3.6 OPERATING SYSTEMS OF IOT DEVICES

A discussion of IoT devices will not be complete without reference to the operating systems of these devices. This section discusses the role of an operating system (OS) in IoT devices, as well as the prevalent IoT-based operating systems in use today. The different sensor nodes discussed earlier come embedded with an OS. In most cases, these nodes run one of the many available versions of embedded Linux. The position of the researcher is that the presence of a specific operating systems impacts the vulnerability of a specific device of appliance.

Silberschatz (2010:3) defines an OS as a program that manages hardware and also provides a basis for applications programs to act as an intermediary between the computer user and the hardware.

The main function of the OS is to manage the allocation of hardware resources to users (Farooq & Kunz, 2011:5901). The hardware which operating systems manage, include processors, memories, timers, I/O devices such as mice and keyboards, communication hardware such as network interface cards, etc. (Farooq & Kunz, 2011:5901). Without an OS, a computer is unusable. What really controls the hardware in an OS is referred to as the kernel. An OS is divided into two sections, the shell and the kernel. The shell provides user interaction with a system, this can either be in command (using a CLI) or Graphic User Interface (GUI) based.

The design of an OS is characterized by the kernel structure, the schedulers, and the programming language used (Baccelli *et al.*, 2013:2453).

The kernel is made up of system functions, mainly written in C, C++, and assembly, that interact directly with the hardware. The kernel is the heart of the operating, comprising of sub-systems such as the central processing unit (CPU) and memory schedulers (Tanenbaum, 2009:94). Every process that runs on a computer requires a number of resources before being able to run. These resources may include the amount of random access memory (RAM) and CPU time required by the process. Management of these resources is vital for optimum functionality of an operating system. For instance, in time-sharing systems, CPU scheduling is really an important part of the OS, in making sure that the CPU is well utilized among the processes. To achieve this efficiency, OSes employ a number of CPU scheduling algorithms such as First in, first out (FIFO), Round Robin (RR), Shortest Job First (SJF), priority, and others to manage CPU time.

Memory is another limited resource in any computer system, hence memory scheduling ensures that one running task does not take possession of all the available memory, depriving other tasks from running in the process (Elkaduwe *et al.*, 2008:36). Thus in many kernel designs, memory spaces that are allocated to one process are protected from other processes by making use of semaphores and locks (Tanenbaum, 2009:79).

Kernel design is crucial in producing an optimum and secure operating system (Rushby, 1981:12-21). Many operating systems have been implemented using various types of kernel structures such

as monolithic, layered, microkernel, virtual machines etc. (Baccelli *et al.*:3; Tanenbaum, 2009:42-51).

In monolithic design, the kernel is created as one piece of code, making it difficult to understand the system at times. The layered approach, on the other hand, tries to divide the OS into layers creating a hierarchy, where a developer can separate the OS between the user space and kernel space. In microkernel design the OS is even divided further into modules. This separation leaves only a few important functions in the kernel (Baccelli *et al.*:3).

3.6.1 IoT based operating systems

Unlike traditional computers that come with gigabytes of RAM and multi-core CPU, the majority of IoT nodes are limited in hardware resources. These limitations make it impossible to make use of the available desktop OSes, such as Linux, for IoT purpose (Baccelli *et al.*, 2013:2453). For instance, some sensor nodes make use of 8-bits microcontrollers, with as little as a few kilobytes of program memory and hundreds of bytes of RAM (Alagupandi *et al.*, 2014:105). Other IoT nodes also run on batteries, thus requiring an efficient usage of energy (Miorandi *et al.*, 2012:1502). In addition, an IoT OS should be reliable, support real-time functionality, support a number of network protocols to allow devices to easily interoperate with the internet, and lastly security should be integrated into the OS itself, should be able to support standard application program interfaces (APIs) such as POSIX, support for common programming language such as C++ (Baccelli *et al.*:2). The design of an IoT based OS should hence be able to take these limitations into consideration. In this section a summary of available IoT OSs will be given, together with the features that each OS supports. The section will consider only three commonly used OSes, namely Contiki, TinyOS, and RIOT.

3.6.1.1 Contiki

Contiki is an open-source operating system designed for IoT devices. It supports a good number of network protocol such as IPv4 and IPv6. It has also support for 6lowpan, RPL, CoAP, which are low-energy communication protocol designed specifically with IoT in mind. Contiki supports a wide range of hardware, a list of these is given on their website (Contiki-os.org, 2016). As discussed in the hardware section, WSN deploys small sensor nodes that may be deployed in environments where it will be impossible to retrieve them again. In this instance, the dynamic loading of code becomes really important. Even after a sensor node has been deployed, it makes it

possible to update the code dynamically (Dunkels *et al.*, 2004:2). For instance, while with other OSes to upgrade a system you will need to generate a new OS image together with application, the design of Contiki allows modules and services to be uploaded at runtime. In most cases these services are very small in size, and for such a limited network as a WSN, this ability makes it a great choice for IoT.

In many multithread operating systems, each created thread is given its own stack. Every time a thread is created, the stack is allocated a memory space that cannot be shared with other threads (Dunkels *et al.*, 2004:3). In memory-constrained sensor nodes, this approach can be a challenge. In multithreaded systems locking mechanisms, such as semaphores are implemented to prevent one thread from accessing another thread's memory space (Silberschatz, 2010:236). To overcome this problem, Contiki is designed as an event-driven operating system. In an event drive OS, a process is implemented as an event handler that can run to completion without disruption since they cannot block. In such an operating system all processes can share the same stack, allowing these processes to share the memory resources among all running processes (Dunkels *et al.*, 2004:3). This is a neat feature, especially for resource-constrained hardware.

3.6.1.2 ***TinyOS***

TinyOS is another version of the embedded OS designed for low-powered embedded systems. The TinyOS wiki page (TinyOS, 2016b) describes the OS as “a scheduler and a collection of drivers for microcontrollers and other ICs commonly used in wireless embedded platforms”. The operating system is written in NesC, which is a dialect of C (Yan *et al.*, 2009:562). The programming model used in TinyOS centres around the concept of components that encapsulate a specific set of services specified by interfaces (Levis *et al.*, 2005:118).

The OS was designed with the following requirements in mind, *limited* resources presented by most hardware used in WSN; *reactive* concurrency which enables the OS to handle real-time tasks for sensing operations; *low* power to allow wireless nodes to use their batteries effectively and for longer time; *flexibility* which allows the OS to be ported to a variety of hardware platforms (Amjad *et al.*, 2016a). The operating has met the requirements for low energy requirement by implementing low-energy communication protocols such as 6LoWPAN and ZigBee (Amjad *et al.*, 2016b:9). Due to the lack of physical memory protection, the OS has implemented various mechanisms to provide memory protection. These mechanisms include Untrusted extension for

TinyOS (UTOS) and Safe-TinyOS (Amjad *et al.*, 2016a:6). To support multitasking capabilities, TinyOS comes with a number of scheduling techniques such as Priority scheduling, Earliest Deadline First (EDF), Real-Time Scheduling (RTS), Deadline Scheduler (DS), Priority-Based Soft Real-time Scheduling, and Adaptive Double-Ring Scheduling (ADRS) (Amjad *et al.*, 2016b:5).

3.6.1.3 RIOT

RIOT started as an operating system for WNS with the main design objectives being reliability and real-time support (RIOT, 2015). RIOT is designed to be an operating system that bridge the gap between mainstream OSes and WNS OSes such as Contiki and TinyOS (Baccelli *et al.*:5).

RIOT is designed to support a number of microcontrollers to microprocessors, from 8bit to 32bit. It partially supports POSIX, with versions to being able for full support. Support of POSIX means applications can easily be ported. RIOT has support for a protocol stack that is cable of providing energy-efficient communication protocols. It supports 6LoWPAN, IPv6, RPL, and UDP. More on RIOT and its comparison to other IoT based OSes can be found in Baccelli *et al.* (2012); Baccelli *et al.* (2013); RIOT (2015).

This section is concluded with a comparison of the discussed operating systems provided in Table 3-5.

Table 3-5 Comparison of Current IoT Operating Systems (RIOT, 2015)

	Min RAM	Min ROM	C Support	C++ Support	Multi-Threading	MCU w/o MMU	Modularity	Real-Time
Contiki	< 2kB	< 30kB	*	✗	*	✓	*	*
Tiny OS	< 1kB	< 4KB	✓	✗	*	✓	✗	✗
Linux	~ 1MB	~ 1MB	✓	✓	✓	✗	*	*
RIOT	~ 1.5kB	~ 5kB	✓	✓	✓	✓	✓	✓
Full support ✓ Partial support * No Support ✗					RAM: Random access memory ROM: Read only memory MCU: Microcontroller unit MMU: Memory management unit			

Since security of is the main focus of the dissertation, security aspects of the operating systems are discussed in the next section.

3.6.2 Security issues in IoT operating systems and applications

The majority of wireless sensor node OSs are highly vulnerable to memory safety problems. For instance, Contiki is known to be affected by this issue because of its extensive use of type casts and pointers (Paul & Kumar, 2009:169). One category of errors that sensor network applications are most vulnerable to, is untrapped memory errors (TinyOS, 2016a). According to Paul and Kumar (2009:169), the major reasons for these untrapped errors are as a result of the (1) easiness to corrupt the operating system code; (2) since memory objects are tightly packed, walking even one element past the allotted space is likely to corrupt the RAM; (3) deployed motes (used as wireless sensor nodes) are difficult to debug, so it can be very difficult to tell when memory corruption is the root cause of a serious deployment problem.

The design of an OS plays a vital role where security is concerned. According to Silberschatz (2010:70), sometimes the lack of a design methodology can leave an OS open to malicious applications that could crash the whole system.

An operating system, as a software, can be susceptible to software attacks just like any other application, but for the fact that an operating system provides an environment where other applications can operate, means that it should provide the first layer of protection.

The purpose of security according to Frustaci *et al.* (2018:2486) is to provide confidentiality, integrity, and availability, thus an operating system should endeavour to provide all of these for all applications and services running on it.

A common coding vulnerability that results from poor programming, is buffer overflow. Often programmers forget to enforce the limit on arrays, buffers and pointers. This results in software code that is more vulnerable to security intrusions exploiting buffer overflow vulnerabilities (Madan, B.B. 2005).

Writing reliable applications for sensor networks is a challenge for programmers, this is mainly due to the fact that severe resource constraints force programmers to use unsafe low-level

languages, hardware-based memory protection is unavailable and, applications are concurrent and distributed (Coopridge *et al.*, 2007:205).

Safety violations on the part of the application programmers can result in an attacker being able to use malicious code to intrude a WSN. According to Francillon and Castelluccia (2008:15), permanent code injection attacks are very powerful when it comes to WSN. In such an attack, malicious code can be injected by an attacker in order to take control of a node. Once the attacker is successful, he can be able to hijack or monitor the network.

3.7 NETWORKS

Connectivity or transmission is one the three layers in an IoT gateway. It is responsible for many of the security vulnerabilities in a smart home. Various types of networks are involved in a smart home and each with its own set of vulnerabilities.

A common understanding of networks is achieved by means of a short discussion of network definitions and classification. Roberts and Wessler (1970:543) define a network as “a set of autonomous, independent computer systems, interconnected so as to permit interactive resource sharing between any pair of systems”.

According to Reid (2008:63), “networks provide the ability to connect people and equipment no matter where they are in the world”. As shown in Figure 3-4, a network comprises of host devices (e.g. computers), media (e.g. cables), network devices (e.g. switches and hubs), and peripherals (e.g. attached scanner) (Reid, 2008:65).

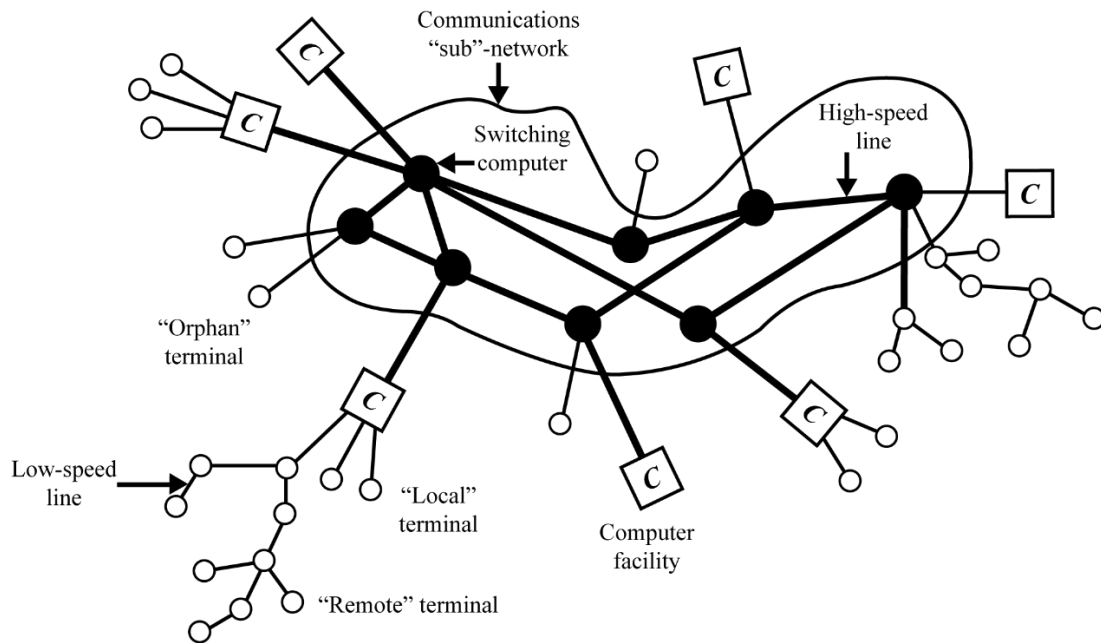


Figure 3-4 Structure of a computer-communication network (Kleinrock, 1976:1327).

The smallest network can comprise of just two hosts, such as two computers connected together, or a cell phone connecting to a laptop using Bluetooth (Reid, 2008:65).

Computers and therefore networks were not always readily available as today. The first sub-section here is devoted to the development of the internet as we know it today, since the internet and internet security are central in a smart home.

3.7.1 Historical development of the internet

Information sharing has always been the core functionality of a computer network since its inception in the 60s (Leiner *et al.*, 2009:23). In those years, a network was limited only to a few organizations, first the Department of Defence in the USA, and later the technology was made available for civilian use. Even though networking could be used by civilians, it was still limited to organizations such as universities. This allowed the universities to experiment and carry more research in the field of computer networks.

With the birth of the computer network, experimentations started on the design of network-based applications. In 1972 electronic mail was introduced (Leiner *et al.*, 1997:103), and this changed

the way information was exchanged. ARPANET was the only network available in the 70s, but it was anticipated that more private networks would be created and get interconnected. This gave way to the development of the internet as we know it today.

The possibility of a network was limited to certain organizations only, because of the lack of personal computers in the 70s. A few personal computers existed as DIY kits and later as off-the-shelf devices, but there was a lack of interest from the masses. Things started to change though with the introduction of the IBM personal computer in August of 1981 (IBM, 2015). With companies wanting to go digital, there was a need to have private networks implemented in any organization with more than one computer in the same building. It was inevitable that computers would have a great impact on businesses, as shown in this study by Osterman (1986:175).

With computers becoming cheaply available in many companies, the true purpose of a computer network began to become apparent. Workmates could share files easily among each other, printers could be networked and shared in a department, thus reducing the cost of having multiple individual printers. File servers allowed the ability to have a central repository of documents that could be accessed by everyone with permission.

The introduction and availability of the internet have been a great game-changer when it comes to the way information is exchanged and shared. The first iteration of the internet, also known as Web 1.0, the emphasis was placed on providing users with information, as Barsky and Purdon (2006:65) put it, “Web 1.0 was all about commerce” and users had no input on what was displayed on websites.

However, a paradigm shift occurred with the introduction of Web 2.0. Not only were users able to get contents from the internet, but they were now able to contribute contents as well. Goodchild (2007:27) describes Web 2.0 as a bi-directional collaboration between the user and the service provider. Wikis are a good example of this technology. Désilets *et al.* (2005:3) describe a wiki as “a collective website where a large number of participants are allowed to modify any page or create a new page using their web browser”.

Another area where Web 2.0 has been greatly utilized is in social networks. From the start, social networks have had one focus only, that of sharing information (Bakshy *et al.* 2012:520). In many instances, social networks have been used as a platform to break the latest news. An example of

this took place in armed conflict areas, such as in the recent conflicts and uprisings in Egypt and Libya (Ali & Fahmy, 2013:59). In a study conducted by Kwak *et al.* (2010:591) on the ability of Twitter as a news media, it was reported that out of all the trending topics that were analysed during a certain time period, 85% of these were news headlines.

The current wave of changes that have been affecting the internet and the way we share information is described by Guo *et al.* (2012:925) as “a technical revolution that represents the future of computing and communication”, the IoT. In the IoT paradigm, devices which will make up the network, will encompass mainly common things in one form or another (Gubbi *et al.*, 2013:1645). Guo *et al.* (2012:925) describe IoT as “the emerging trend of augmenting physical objects and devices with sensing, computing, and communication capabilities, connecting them to form a network and making use of the collective effect of networked objects”.

The vision behind IoT is to move from the traditional internet that connects end-user devices, to one that connects physical objects to the internet so that they can communicate with each other or with humans (Miorandi *et al.*, 2012:1498) and cooperate to reach a certain goal (Atzori *et al.*, 2010:2787).

In their research, Guo *et al.* (2012:926) acknowledge that data sharing is the major area of IoT. From its inception, the function of a network has remained the same, that of information sharing. In this research, the main focus will be on IoT.

In the next section different categories of networks are discussed.

3.7.2 Categorisation of networks

Networks can be categorised based on their methods of connection. The two common categories are wired and wireless networks. The selection of one technology over the other, depends on many factors such as hardware requirements, range, mobility, reliability, security, as well as the benefits (Navpreet & Sangeeta, 2014:34). Table 3-6 provides a comparison of the two technologies based on their characteristics.

Table 3-6 Characteristics of wired and wireless networks (Navpreet & Sangeeta, 2014).

	Wired networks	Wireless networks
Mobility	Limited (operates only on connected computers linked with network)	Outstanding (enable wireless user to connect to network and communicate with others anytime, anywhere)
Reliability	Ethernet cables, switches are reliable because manufactures have improved technology over several decades	Reasonably high (because if the major section like router breaks down the whole network will be affected)
Medium	Copper or Fibre optic cables	Radio waves
Security	Good	Weak (because wireless communication signals travel through the air and can easily be intercepted, which can be improved by encryption technique.
Cost	Less (such as Ethernet cables and switches are not expensive)	More (wireless adapters and access points are quite expensive)
Quality of service	Better	Poor (due to higher jitter, delays and longer connection set up times)
Types	Local Area Network (LAN) Metropolitan Area Network (MAN) Wide Area Network (WAN)	Wireless networks can be classified in terms of different characteristics: By network formation and architecture: • Infra structure-based network • Infra structureless (ad hoc) network By communication coverage area: • Wireless Local Area Network (WLAN) • Wireless Metropolitan Area Network (WMAN) • Wireless Wide Area Network (WWAN) • Wireless Personal Area Network (WPAN) • Wireless Sensor Network (WSN) By access technology: • Global System for Mobile Communications (GSM) Network • Time-division multiple access (TDMA) Networks • Code-division multiple access (CDMA) Networks

Common categories of networks include telephone and cellular networks, i.e. 3G, GPRS, 4G, LTE, and PSTN; industrial networks, i.e. PROFINET, PROFIBUS, CAN, INTERBUS, etc.; satellite networks; computer networks (i.e. LAN, WAN, MAN, WLAN, WPAN); and Wireless Sensor Networks (WSN).

With all these different types of networks, many service providers had to rely on multiple overlaying networks to provide parallel services such as voice, Frame Relay, and internet access (Zhou *et al.*, 2003:316). The quick advancement in technology made it possible to have networks that offer data, voice, and multimedia services over a single IP infrastructure (Geer, 2005:14). Reid (2008:64) describes this IP infrastructure as a *converged network*.

With regard to this study, the focus is on a LAN since a HAN is a specific type of a WLAN.

3.7.3 Local Area Network

A LAN is a type of network that is limited to a certain geographic location (Clark *et al.*, 1978; Teare, 1999), connecting computers, servers, printers and other network devices together in a setup which allows easy sharing and resource access (IBM, 1996). In a LAN, devices are connected or organized in different ways, this organization is referred to as topologies. Topologies are logical architectures of how computers interconnect, and not a physical one. Four different topologies exist for LAN, namely bus, star, ring, and tree topology (Clark *et al.*, 1978; Teare, 1999).

3.7.3.1 LAN communication

To better understand how communication takes place in a network, it is important to understand the rules that govern this communication. Data within a network is carried from one host to the other through the use of a Protocol Data Unit (PDU). A PDU is simply a unit of communication within a LAN (Cisco Network Academy, 2015). The Encyclopedia Britannica (2015) defines a network protocol as “a set of rules or procedures for transmitting data between electronic devices, such as computers. In order for computers to exchange information, there must be a pre-existing agreement as to how the information will be structured and how each side will send and receive it”.

LAN protocols operate at the bottom of the last two layers of the OSI model (Teare, 1999). The OSI reference model is a hierarchical representation of how protocols interact. IBM (1996) refers to it as “an excellent model to understand how networks work”.

3.7.3.2 *The OSI Model*

The OSI model comprises of 7 layers that demonstrate protocol interaction in a network. These layers are, *Application*, *Session*, *Transport*, *Network*, and the *Physical* layer.

- I. *Application Layer*: Communication in a LAN is initiated by an application on a host computer in a network. For instance, when a user wants to access a website, he would normally type the URL of the site in the browser. In the application layer, the browser will then make use of Hypertext Transfer Protocol (HTTP) to format the request and forward it to the next layer.
- II. *Presentation Layer*: The presentation layer will make sure data coming from the application layer is converted, compressed, and encrypted before forwarding it to next layer.
- III. *Session Layer*: The session layer allows session establishment between processes running on different computers (Microsoft, 2015b). It creates, manage and terminate these sessions.
- IV. *Transport Layer*: The transport layer receives messages coming from the session layer and breaks it into segments of equal sizes and prepends a header to each section. This header information contains a segment number or sequence number, which will allow the recipient to rebuild the packet.
- V. *Network Layer*: In the network layer each segment coming from the transport layer is placed in a container (IP packet), where both the destination and source IP addresses are added. This process is known as encapsulation.
- VI. *Datalink Layer*: The data link layer receives the IP packet from the network layer and encapsulates it into an Ethernet frame. In the Ethernet frame both the source and destination MAC addresses added (Microsoft, 2015b).
- VII. *Physical Layer*: The physical layer's function, is to convert any information it receives from the data link layer, from binary to either electromagnetic, radio wave or light depending on the medium the data needs to be transmitted out of the PC (Cisco Network Academy, 2015).

When the receiving host gets the process takes place in reverse order. Starting with converting the signal back into binary data, then the data link layer will determine to which computer on the network it must forward the Ethernet frame to, based on the information in the destination MAC field.

Computers on the same LAN communicate by means of Media Access Control (MAC) address. A MAC protocol is a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) (Anon, 2012) used LAN. When a network device wants to transmit data on the network, it checks first to see if the medium is free and no other devices are transmitting. If another device is transmitting, it waits for a certain time period before it tries again. If two hosts get access to the medium and start transmitting at the same time, collision will take place. Once the collision is detected by both hosts, they will both back off and wait for a time period before they try again (Cisco, 2015).

A MAC address, also known as the physical address, is a 48-bit address often written in hexadecimal notation (i.e. 08-00-7B-B0-C0-5B). This address is hard-coded on each network card of a network node, and it cannot be changed. The MAC address uniquely identifies each computer in LAN communication. LAN communication makes use of Ethernet as a standard to define how information is coded, transmitted over a medium. Ethernet operates at the data link and physical layers of the OSI model. In a LAN where Ethernet is used, a copper cable is usually the medium used to interconnect nodes. The Institute of Electrical and Electronics Engineers (IEEE) document on Ethernet standard (Anon, 2012) describes in detail the functionality of this standard. Ethernet is well known by its standard name of IEEE 802.3.

3.7.4 Wireless Networks

Wireless networks come in various types, supporting different data transmission rates, range covering, power usage, and operating at different frequencies, as shown in Table 3-7. This classification enables designers of IoT to select the best protocol for their application. For instance, due to the limitation of battery on most IoT sensor nodes, designers have opted to go with the IEEE 802.15.4 as a communication protocol in wireless personal area networks (Atzori *et al.*, 2010:2791). Other IoT objects make use of protocols such as ZigBee and Z-Wave. This interoperability IoT protocol has spearheaded the development of smart IoT gateways (Shang *et al.*, 2013:720) which are able to control traffic from a multitude of devices in a smart home using different transport protocols. A smart home comprises also of smart devices/appliances that are

not battery operated, hence they may not have the power limitations of battery-operated IoT objects. These may include, smart fridges, smart speakers, and smart TVs which are connected to the power mains. These devices come equipped with Wi-Fi connectivity. Smart objects such as, smart door locks or smart water leakage detectors may come equipped with a protocol such as ZigBee. The next sections discuss in brief two wireless technologies that are likely to be found in a smart home, Wi-Fi and ZigBee.

Table 3-7 List of wireless protocols (Postscapes.com, 2019)

Technology	Frequency	Data Rate	Range	Power Usage	Cost
2G/3G	Cellular bands	10 Mbps	Several miles	High	High
Bluetooth/ BLE	2.4 Ghz	1, 2, 3 Mbps	~300 feet	Low	Low
802.15.4	subGhz 2.4 Ghz	40, 250 kbps	>100 square miles	Low	Low
LoRa	subGhz	<50 kbps	1-3 miles	Low	Medium
LTE Cat 0/1	Cellular bands	1-10 Mbps	Several miles	Medium	High
NB-IoT	Cellular bands	0.1-1 Mbps	Several miles	Medium	High
SigFox	subGhz	<1 kbps	Several miles	Low	Medium
Weightless	subGhz	0.1-24 Mbps	Several miles	Low	Low
Wi-Fi	subGhz 2.4 Ghz, 5Ghz	0.1-54 Mbps	<300 feet	Medium	Low
WirelessHart	2.4 Ghz	250 kbps	~300 feet	Medium	Medium
ZiBee	2.4 Ghz	250 kbps	~300 feet	Low	Medium
Z-Wave	SubGhz	40 kbps	~100 feet	Low	Medium

3.7.4.1 *Wi-Fi*

Wi-Fi, also known as IEEE 802.11, was designed to overcome the limitations that cables place in setting up networks. WLAN is not a replacement of the wired version, rather more of an extension

allowing clients to connect wirelessly to a LAN. It was designed to offer higher data rates using the unlicensed frequency spectrum (Hyeyeon *et al.*, 2007:184). IEEE 802.11 provides a number of standards referred to as a, b, g, and n. These categories of the standard provide wireless data transfers from 10 Mbps to 600 Mbps (Jun-Hyuk *et al.*, 2013:761).

Table 3-8 describes the IEEE 802.11 standard, including the various categories, transmission speed, and the frequency at which they operate.

Table 3-8 Categories of IEEE 802.11 standards (Pi Huang, 2016).

Standard	Release date	Band (GHz)	Bandwidth	Maximum Data rate
802.11	1997	2.4	20	2 Mbps
802.11b	1999	2.4	20	11 Mbps
802.11a	1999	5	20	54 Mbps
802.11g	2003	2.4	20	54 Mbps
802.11n	2009	2.4 & 5 GHz	20,40	600 Mbps
802.11ad	2012	60	2160	6.76 Gbps
802.11ac	2013	5	40,80,160	6.93 Gbps

In a WLAN, a Wireless Access Point (WAP) is used as a central connection point for all Connecting wireless clients or stations (Mishra & Arbaugh, 2002:2). For a WLAN to be fully operable, a Service Set Identifier (SSID), Dynamic Host Configuration Protocol (DHCP), and security will need to be configured. An SSID is a case sensitive alphanumerical string that is sent in the header of frames transmitted over the WLAN. It identifies each wireless client's network (Reid, 2008:240). The DHCP server distributes IP addresses dynamically to wireless clients. When configuring a WLAN, a decision should be made on whether access will be open or closed. For instance, in an open area such as an airport, the majority of the wireless hotspots are open, hence do not require one to authenticate. For private's WLAN though, the requirements are different.

Most private WLANs require a level of authentication to protect the information on the network. For instance, a user would need to enter a password or key, depending on the settings on the WAP, in order for him to be authenticated. Once authenticated, the WAP will then open the channel allowing the client access to the network resources.

3.7.4.2 ***ZigBee***

Zigbee, currently at version 3 (Zigbee.org, 2019), is a protocol stack for IoT developed by the Zigbee alliance. The protocol stack is built on a number of layers as shown in Figure 3-5. The base of the protocol stack relies on the IEEE 802.15.4 transport standard, which is a transport standard for Low-Rate Wireless Personal Networks (LR-WPANS)(Narmada & Rao, 2012:178). The other layers include the security service layer, the network layer, and an application layer which were created by the ZigBee alliance. According to Narmada and Rao (2012:178) Zigbee is designed to be used for remote controls and sensor applications, especially in areas with harsh radio reception and remote locations. These characteristics make ZigBee a good candidate for home area network applications. Although other protocols exist that can be used, as shown in Table 3-7, they have limitations such as short-distance or requiring clear line-of-sight. These limitations may cause a problem in a home with walls and furniture, making the establishment of connectivity among devices difficult (Narmada & Rao, 2012:179).

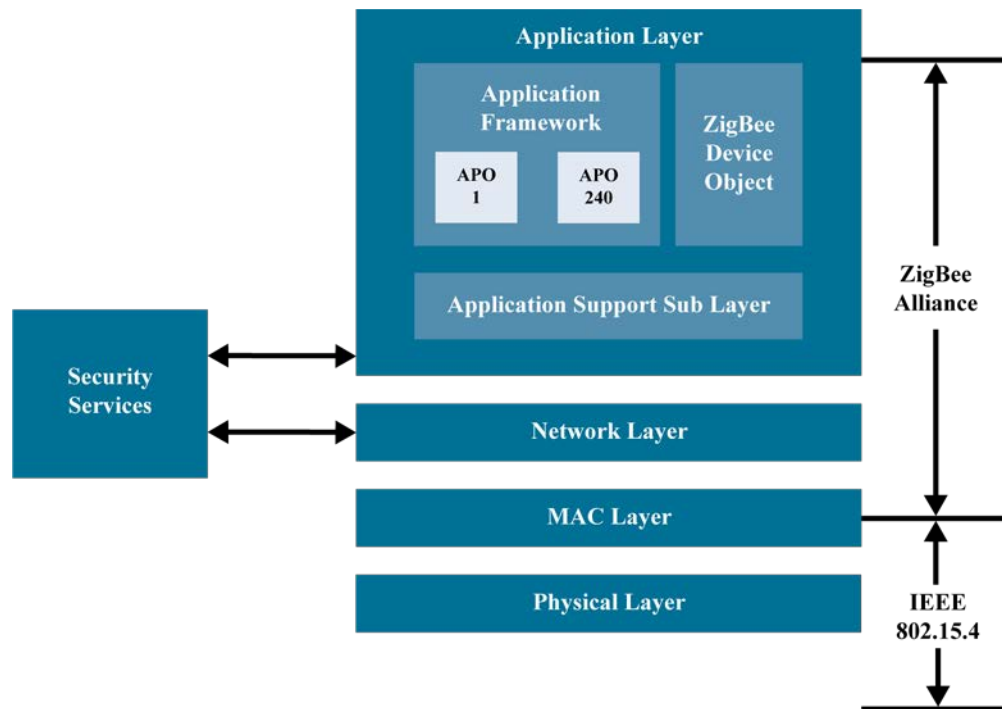


Figure 3-5 ZigBee protocol stack (Anon, 2011; Ramya et al., 2011:299)

A ZigBee network as shown on Figure 3-6 comprises of three main components, a ZigBee Coordinator (ZC), a ZigBee Router (ZR), and ZigBee End Devices (ZED) (Varchola & Drutarovský, 2007:3).

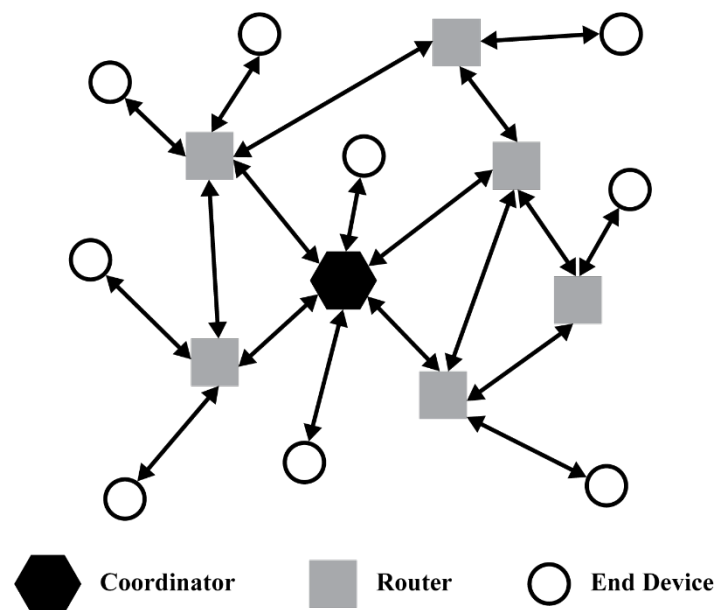


Figure 3-6 ZigBee logic topology (Varchola & Drutarovský, 2007)

- I. *ZigBee Coordinator (ZC)*: At the core of a ZigBee network is the ZC. According to Somani and Patel (2012:29), the ZC is responsible for the initialization of the network by selecting parameters such as network channel and unique network identifiers. There is one ZC per network. In addition to setting these parameters, the ZC also stores security keys and other network information (Varchola & Drutarovský, 2007:29)
- II. *ZigBee Router*: A router can be used in LAN to interconnect multiple subnets. In a ZigBee network the router plays quite a different role, it acts as an intermediary device transmitting traffic from one node to another (Somani & Patel, 2012). End devices connect directly to a router as shown in Figure 3-6, and to extend a ZigBee network, one needs to add extra routers.
- III. *ZigBee End Device*: A ZED can be low-powered or battery-operated devices equipped with sensors for the purpose of collecting data (Ramya *et al.*, 2011:298). These devices can relay data to the parent node such as the coordinator or router but cannot send relay data to other end devices.

The functionalities of ZigBee protocol stack sublayers are based on the OSI model and can be described as:

- I. *MAC layer*: The IEEE 802.15.4 standard defines the MAC and physical layers (Narmada & Rao, 2012). According to (Chandane *et al.*, 2012), the MAC sublayer is responsible for the transmitting and receiving of MAC protocol data units (MPDU). Some functionalities of the MAC sublayer include beacon management, channel access, frame validation, acknowledgement of frame delivery and more (IEEE, 2006).
- II. *Physical layer (PHY)*: According to IEEE (2006:17), the PHY layer plays two roles, it provides data services and management service. The PHY data service is responsible for the transmission and reception of the PHY protocol data unit (PPDU) across the radio channel. The PHY layer supports three frequency bands, 2.4GHz, 915Mhz, and an 868MHz. These bands support 16, 10, and 1 channel respectively (Ramya *et al.*, 2011:299).
- III. *Network layer (NWK)*: The network layer is responsible for the routing and formation of a network packet. By making use of routing tables, routers and coordinators are able to forward information from one node to another by selecting the correct path to the

destination node. As devices join or leave the network, routers/coordinators are able to maintain the correct topology of the network (Somani & Patel, 2012). Routers and coordinators are also responsible for route discovery in the network (Ramya *et al.*, 2011:299).

- IV. *Application support sublayer (APS)*: The application layer is the topmost layer of the stack as shown in Figure 3-5. It hosts three sub-layers, the application object sub-layer which controls the protocol layer in Zigbee devices; the ZigBee device object sub-layer which is responsible for service discovery, security, and binding; and lastly the application support sub-layer which provides an interface between the application layer and the network layer. According to Somani and Patel (2012:32), the APS processes incoming and outgoing data frames to ensure they are transmitted securely.
- V. *Security services*: The security services layer provides security services to both the network and application sublayers as shown in Figure 3-5. According to Ramya *et al.* (2011) the security services provide methods for establishing security keys, transportation of keys, protection of data frames, as well as management.

3.7.5 Security in wireless networks

Wireless networks are susceptible to several attacks; in this section, security implementations of Wi-Fi and ZigBee protocols are discussed.

3.7.5.1 Wi-Fi security

The introduction of WLAN came with several security concerns. Despite its convenience, WLAN is comparatively weak from a security perspective (Xiong & Jamieson, 2013:441). With more devices connecting to the network wirelessly, security has become a prominent concern for individuals and companies alike (Sagers *et al.*, 2015:5453). There are two problems that WLANs experience, first because WLAN makes use of radio broadcasting, this makes it vulnerable to eavesdropping. Secondly, an attacker does not require physical access to the WAP for him to gain access to the network (Buttyán & Dóra, 2006:2). The following sub-sections describe methods that are currently being used to provide Wi-Fi security. More detailed explanation on security is provided in Chapter 4.

Authentication

Authentication is a method of controlling who connect the WLAN. WAPs employ three types of authentication, Open, Pre-Shared Keys (PSK), and Extensible Authentication Protocol (EAP) (Reid, 2008:251-252).

When using *PSK authentication*, both the wireless client and the WAP should be configured with the same key. During the authentication process, the WAP sends strings of bytes to the client. Upon receiving this, the client will encrypt this string using a preconfigured encryption algorithm and send it back to the WAP. The WAP will also carry out its own encryption using the same algorithm and the result of this operation will be compared to the encrypted string received from the client. If the two encrypted strings are the same, the client is then given access to the WLAN (Reid, 2008:251). PSK authentication is designed to be a one-way authentication mechanism, meaning the host is authenticated to the WAP, and not vice versa. To overcome this limitation, EAP was designed. EAP was designed to provide a dual authentication process. EAP works together with a backend server known as Remote Authentication User Service (RADIUS) (Blanco & Marco, 2003:1).

The RADIUS server contains a database of users and their passwords. Once a user wants to connect to the WLAN, the WAP will forward the request to the RADIUS server for authentication. Once authenticated, the WAP can then open the channel allowing the wireless client access to the network (Reid, 2008:252).

Encryption

Encryption is defined as “the process of transforming plain text into cipher text in order to conceal its meaning and so preventing any unauthorized recipient from retrieving the original data” (Mousa & Hamad, 2006:44), thus even when this data is intercepted, it will be unusable (Reid, 2008:253). Authentication can prevent an attacker from gaining access to the WLAN, but it will not stop him from eavesdropping on the communication taking place within the WLAN.

The first encryption method used in WLAN is WEP, which stands for Wire Equivalent Protocol. WEP was designed to offer privacy for network traffic using wireless protocol (Arbaugh *et al.*, 2002:6). WEP utilizes a 64bit or 128bit key. In a 64bit key, the 40bit is used for the shared key and the remaining 24bit is for Initialization Vector (IV). This key is used to initiate the RC4 algorithm (Rowan, 2010:10). RC4 is an encryption algorithm utilized in WEP (Mousa & Hamad,

2006:49). RC4 uses the same key for encryption and decryption. It uses a short seed value to produce a long string of pseudo-random characters sequence. This sequence is then XORed with the plain text to produce the encrypted message (Buttyán & Dóra, 2006:3; Mousa & Hamad, 2006:49).

WEP was not a very secure way of protecting a WLAN. A number of vulnerabilities were discovered in its design and implementation (Buttyán & Dóra, 2006:5). For instance, according to Rowan (2010:10), WEP can be cracked in 5 minutes to half an hour depending on the strengthening of the network being hacked.

To overcome the shortfall of WEP, two standards were created, Wi-Fi Protected Access (WPA) and WPA2. WPA still continues to use RC4 algorithm, with improvement on the IV length which has been doubled from 24bit to 48bit, and the key to 128bit. WPA has also introduced another layer of security named MIChael, which provides protection from replay attacks (Rowan, 2010:10). WPA makes use of Temporal Key Integrity Protocol (TKIP) to manage keys and avoid duplication (Perez & Mahdy, 2008:3). Another encryption method supported by WPA is the Advanced Encryption Standard (AES). WPA/WPA2 has also suffered a number of network attacks, and a few vulnerabilities in their design have been discovered (Ahmad, 2010:1-5). Encryption is discussed in the next chapter.

3.7.5.2 *ZigBee security*

ZigBee networks are susceptible to various network attacks, just like any other computer network. Frequent attacks may include eavesdropping, DoS, node compromise, sinkhole or wormhole attacks, and physical attacks (Karnain & Zakaria, 2015:2). Protection must be provided for both devices and the network. ZigBee provides built-in security mechanisms to provide security (Yang, 2009:426). Due to the hardware limitations of WSN nodes, ZigBee employs AES-128 encryption algorithm (Yang, 2009:426). As shown in Figure 3-7 security measures are applied to the network layer and application layer. According to Li *et al.* (2010:494) ZigBee provides the following security features:

- *Sequential freshness*: this is a security feature that uses “an ordered sequence of inputs” to prevent frame replay attacks.
- *Frame integrity checking*: ZigBee uses a message integrity code (MIC) to ensure that the data is not modified by an unauthorised person.

- *Entity authentication services*: this service offers a safe way for one node to synchronize information with another node on the network, at the same time providing authenticity built on a shared key.
- *Data encryption*: ZigBee makes use of AES to encrypt communication among nodes in the network, providing protection against eavesdropping.

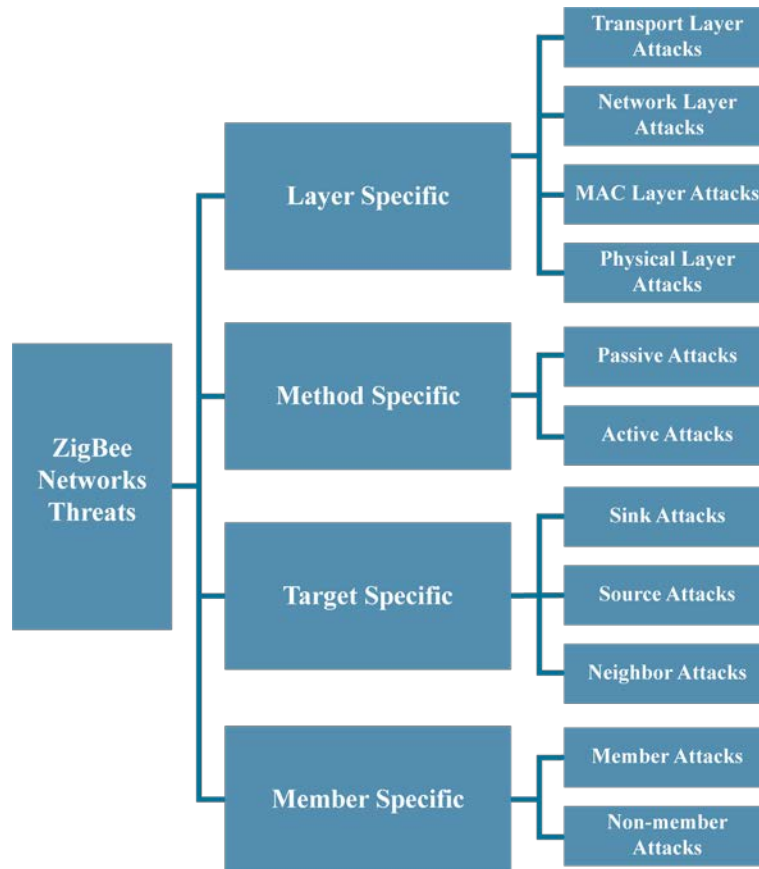


Figure 3-7 Overview of security threats in a ZigBee network (Karnain & Zakaria, 2015:2)

The following section presents an initial reflection on the security implications of the components used in a smart home to take forward in the study.

3.8 SECURITY IMPLICATIONS FOR SMART HOMES

The aim of the chapter is to provide technical background for the components of a smart home in order to provide a theoretical foundation for the empirical investigation. From the literature review, an intuitive perspective of security vulnerability is that the vulnerability is not the first place inherent to the appliance but rather results from the add-on hardware that makes the appliance smart. This implies that a washing machine is not vulnerable, but a smart washing machine is, due to the presence of sensors and internet connectivity. The components required to transform appliance into a smart appliance and a home into a smart home form can be viewed from an architectural perspective in order to provide generalisation beyond specific appliances.

A smart home or IoT can be described in terms of a four layered architecture presented by Vijayalakshmi and Arockiam (2016:34) as:

- The *perception layer* which is responsible for collecting environmental data. This consists of wireless sensors, actuators, and RFID;
- The *network layer* provides routing and transmission of data collected from the perception layer;
- The *support layer* which comprises of cloud and fog computing, provide the support for hosting IoT applications which can be accessed by resource-constrained devices via the internet;
- The *application layer* provides users with IoT services of different kinds according to needs.

In this chapter, the technical discussion frequently leads to an intuitive identification of security vulnerabilities. The IoT architecture model can be used to structure this list of intuitively identified vulnerabilities as presented in Table 3-9. The table is compiled as conclusion for this chapter. Section numbers are provided of discussions from this chapter which provide the theoretical foundation for the identification of the vulnerabilities.

Table 3-9 Intuitive identification of vulnerabilities based on IoT network architecture

Component	Vulnerability
Application layer	
Appliance user interfaces (Section 3.2)	Smart appliances have specific settings which can be manipulated by the user. This is inherently an advantage and threat as described for gateways.
Gateway user interfaces (Section 3.5)	Once again, a user interface creates opportunities for control of security settings but also vulnerabilities due to lack of knowledge by the user. Unauthorised access might be possible.
Mobile user interfaces (Intuitive at this stage)	Mobile device applications pose many vulnerabilities to the home owner. Security concerns are discussed in the following chapter. The application programs to control the hub including the mobile application creates vulnerabilities since RFID can be simulated and other malicious command can be generated by potential attackers.
Support Layer	
Connection from gateway to cloud (Section 3.7)	Connection to the internet creates vulnerabilities.
Cloud service provider (Section 3.7)	Data storage by service provider also has vulnerabilities and might be subject to attacks.
Network Layer	
Connection of sensors to Gateway (Sections 3.4 and 3.7)	Each sensor and its node use specific protocols to connect to the gateway.
Gateway Configuration (Section 3.5 and 3.7)	The ability of the user to manipulate security settings of gateways is both an advantage and vulnerability. It is an advantage when the user has enough knowledge of hardware, but when a user is not knowledgeable it becomes a vulnerability.
Gateway operating system (Sections 3.6 and 3.7)	The sophistication of the operating system used by the gateway creates specific vulnerabilities.
Gateway hardware capacity (Section 3.5 and 3.7)	Aspects such as processor power and memory capacity influence the ability of the gateway to implement security measures and encryption.
Gateway mobile connection (Section 3.5 and 3.7)	The connection between the mobile phone and the gateway has inherent network vulnerabilities.
Perception layer	
Sensors	
Image sensors: Camera and video camera (Section 3.4)	Images and videos are potentially captured without the knowledge of the homeowner and stored on the device or transmitted to the cloud.

Sound sensor: microphone (Section 3.4)	Sound clips are recorded, and potentially can be duplicated for remote voice activation of control devices.
Temperature / light sensors (Section 3.4)	Environmental conditions can be manipulated to achieve specific outcomes.
RFID tags (Section 3.4.5)	The tags of sensors can be simulated or duplicated to gain unauthorised access.
Sensor Nodes	
Nodes and small computers (Section 3.4.2)	Due to size and cost factors the hardware capabilities are insufficient to support traditional operation systems and network protocols, leaving these devices vulnerable to attacks.
Sensor node operating systems (Section 3.6)	The appliances and hubs are loaded with operating systems to control the hardware. Due to size and cost considerations these operation systems are not on the same standard as PC operating systems in terms of security considerations. These smaller operating systems are vulnerable to code attacks and memory errors which may be exploited.
Smart electricity management	
Smart meters (Section 3.3)	Communication between smart meter and utility supplier could jeopardise the privacy of the homeowner in that the communication could identify when the homeowner is not at home.

From the table it is evident that network layer security is an important aspect in IoT security. The next chapter is devoted to network security in order to provide theoretical insights in matters such as encryption and authorisation.

3.9 SUMMARY

The chapter has introduced the concept of IoT and the components of a smart home. Smart homes comprise of various crucial parts, the smart devices (appliances and objects) and the smart gateway that interconnects all these devices, allowing them to easily communicate despite the different protocols they may be using.

The smart appliances and devices discussed, come equipped with various types of sensors which allow these devices to collect data. At the core of these devices, is the operating system which controls the hardware in terms resource management and network connectivity. The various IoT parts discussed present different vulnerabilities to a HAN where they may be used. For instance, the many sensors which are installed in these smart devices, such as microphones or cameras, may put home owners at risk should such sensors be compromised by an attacker.

The operating systems driving these smart devices may possess vulnerabilities that attackers may exploit getting access to vital data. The majority of IoT devices may lack in-built defence mechanisms, so the network may be the only defence to such devices. Any vulnerabilities that may exist in the network itself means that all devices in the HAN may be exposed to attacks. On the other hand, vulnerabilities that may exist in just one device (either in software or firmware) can put the whole HAN at risk of attacks.

It is argued in this chapter that smart appliances and devices are design according to a comparable layered architecture. All these devices have a perception layer for the sensors, and a network layer for connectivity. Some devices have additionally, a supplier layer for internet and cloud support and an application layer for user applications. The discussion was concluded with a list of vulnerabilities possible in each of these layers. This list is taken forward in the study to guide the following chapters.

In the next Chapter, traditional computer security measures are discussed in context home area networks.

CHAPTER 4 SECURITY IN A HOME AREA NETWORK

4.1 INTRODUCTION

The main purpose of this study is to identify security threats posed by smart home devices to unsuspecting homeowners in relation to their privacy in a home area network. The objective of this chapter is to review literature on network security in order to identify threats to homeowners and to guide the empirical study. In order to create a common understanding frequently used concepts are defined in this introduction.

Schneider (2012:14) defines computer security as “*a principle that is concerned with the protection of networks and computers from threats and ensuring trusted access to resources*”. Network security is a subset of computer security. A vulnerability can be viewed as a flaw in the design of a software or hardware that may result in compromising or exposing a system to exploitation (Anjum & Mouchtaris, 2007:7). When a vulnerability is discovered, it makes it easy for an attacker to plan his next action which is to exploit these vulnerabilities (Weber, 2010a). A threat is defined as the “*potential for a security violation, such as the discovery of a vulnerability*” (Silberschatz *et al.*, 2018:642). According to this definition, vulnerability becomes a threat once it has been discovered by an intruder. Threats can be human-made, such as an insider threat (Stewart *et al.*, 2012:724), or as a result of poor hardware design (Canonical, 2017:6). A discovered threat may lead to an attack by intruders.

Computer security has changed in the past decade. No longer are only computers connected to a network, today we have mobile devices, cars, IoT devices, smart homes and many more network-enabled devices (Easttom II, 2019:3). With so many new devices becoming network and internet-capable, new types of security threats are sure to emerge resulting from specific limitations of the devices used in an IoT network. Although IoT seems to be a very active area of research, very little has been published concerning security (Ali *et al.*, 2019:2).

According to Ali *et al.* (2019:1), achieving proper IoT security is a big challenge today due to the heterogeneity of the technology, since IoT is a blend of old and new technologies trying to work together, and each of these technologies already has its own series of security problems.

Chapter 3 of this dissertation introduced IoT with the opportunities it presents to home users. With IoT fully implemented, billions of devices and things will be network capable, easy to track and remotely monitored over the internet. As promising as the future of IoT may appear, the idea of remote controlling home appliances or tracking of objects has raised public concerns in many areas (Atzori *et al.*, 2010:2801). A list of intuitive vulnerabilities was provided in the previous chapter to guide this security focused literature investigation as well as the empirical investigation presented in the next chapter.

The chapter starts with positioning IoT network security in context of computer security in Section 4.2. This done in terms of hardware, software and network security all influencing data security. From the discussion in Chapter 3, it became clear that an IoT network has particular traits that make it susceptible to a large number of attacks based on threats and vulnerabilities. The specific heterogeneous nature of IoT and the resulting vulnerabilities are discussed in Chapter 3, Section 3.8 considered from the architectural perspective. The same architectural model is used in Section 4.3 to identify IoT vulnerabilities, threats and attacks from literature on IoT security. Whether data is in rest or in motion, cryptography may be used to protect the data and therefore, the owner of the data. The evolution of cryptography is discussed in Section 4.4 from its inception until modern methods used in IoT networks.

In order to guide the empirical investigation, the chapter presents in Section 4.5, an updated version of the list of vulnerabilities created in Chapter 3, Section 3.8, organised according to the layered architecture of an IoT network.

4.2 IOT IN CONTEXT OF TRADITIONAL COMPUTER SECURITY

The chapter starts with reflecting on IoT security in context of traditional computer security. Computer security encompasses the protection of everything that is found in a computer system environment, this includes hardware, software, networks, as well as data. Figure 4-1 shows how the various aspects of computer security intersect, with the main focus being data security.

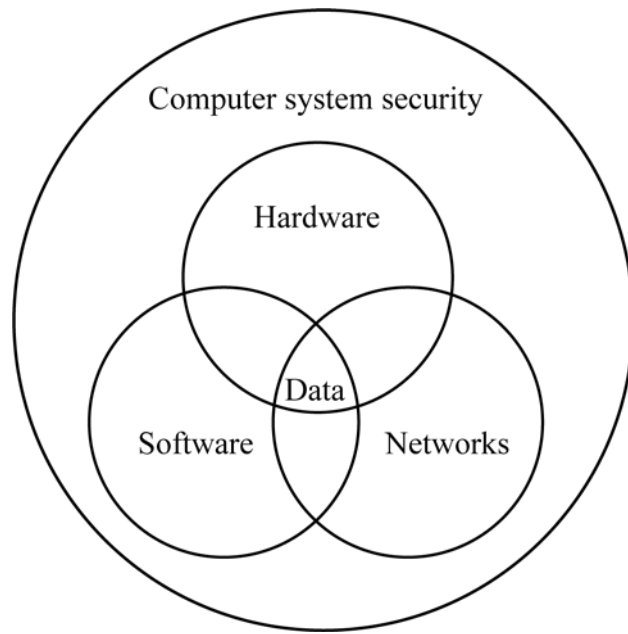


Figure 4-1 Aspects of computer security, adapted from (Carroll, 2014:8)

The core function of every secure system, according to Fisch *et al.* (2017:2) is to provide confidentiality, integrity, and availability. Bhaskar (2008:14) goes even further at defining what security is, by dividing the concept into computer security and network security. He describes computer security as mechanisms and procedures taken to provide confidentiality, integrity, and availability of the data stored on a computer. The components of Figure 4-1 are used to provide structure to this section of the chapter on traditional security and IoT networks.

4.2.1 IoT in context of hardware security

Traditional IT devices, such as computers, can provide security goals to users mainly because they are open systems, meaning users can install security software to provide such goals. Compared to traditional hardware, IoT devices, which are mostly closed systems, on which users cannot install any security software is inherently more vulnerable. Hence, Frustaci *et al.* (2018:2486) argues that security for these devices must be built-in from their design. Another limitation of IoT devices, is that they are resource-constrained, thus only limited security can be built into the hardware itself. Unfortunately, with the rush to get products to the market, the security of IoT devices is being neglected by manufacturers according to Frustaci *et al.* (2018).

A typical home area network may consist of smart appliances, smart sockets, smart lights, security systems smart locks, smart TVs, smart wearable devices etc. (Ali *et al.*, 2017). All these IoT objects are network capable, allowing them to be remotely accessed and operated, thus making them all susceptible to attacks. In 2016 it was reported that the Mirai malware infected a number of IoT devices, including baby monitors, IP cameras, residential gateways etc. These objects were part of a botnet that was used to mount a DDoS attack on large internet companies such as Twitter, VISA, PayPal, etc. (Frustaci *et al.*, 2018:2483).

From this list, it is clear that a typical HAN may consist of a number of smart devices and objects, all of which can be vulnerable in one form or another. Although some of these devices may have been designed with security in mind, but to have just one insecure device in a network may present significant vulnerabilities (Patton *et al.*, 2014:232) and may just be the weakest point for the whole network.

4.2.2 IoT in context of software security

Software security focuses on the design of software that can withstand malicious attacks (McGraw, 2004:1). According to Takanen *et al.* (2018:2), every software system has security issues and can be compromised. They discuss a method called fuzzing, which they use to find security flaws in a software. Pfleeger and Pfleeger (2012:89) categorise program flaws that may result from poor coding as follows:

- Domain error: controlled access to data
- Validation error (incomplete or inconsistent): permission checks
- Serialisation and aliasing: program flow order
- Inadequate identification and authentication: basis for authorization
- Boundary condition violation: failure on the first or last case
- Other exploitable logic errors

Since the beginning of smart phones with touch screens, the software spectrum has changed tremendously. With over 3.3 million smart phones in circulation (Market.us, 2019), apps stores, such as Google's and Apple's, host millions of applications (Sharma, 2019). Unfortunately many of these mobile apps come with vulnerabilities that users are mostly unaware of (Leavitt, 2011:11). IoT rely greatly on software, both in the form of firmware and mobile applications. The majority

of software used in developing IoT devices and services are open source, such as the Linux kernel and other source codes. Due to their open source nature, some of these tend to have security flaws (Wang *et al.*, 2018:2). Thus, some IoT software are designed with security flaws at their core. This was the case with many Samsung software systems, including their Tizen OS which is based on the Linux kernel (Paul, 2017). All these mobile apps rely heavily on the internet, the same is true for software used IoT devices. Due to the lack of processing power in most of them, these devices are designed to connect to a network so that they can transmit data to the cloud for processing. Thus, the security of mobile apps is intertwined with network security to prevent illegal access.

4.2.3 IoT in context of data security

In the centre of Figure 4-1 is data security since protecting data is the main objective of computer and network security. Data security involves the protection of sensitive data in order to avoid theft and protect privacy (MIT, 2016). Not all data is sensitive, hence it is important to have data classified. Stewart *et al.* (2012:225) describes the primary objective of data classification is to provide security mechanisms for storing, processing, and transferring of data. Data can be classified based on its sensitivity, cost, risk, vulnerability and many more. In Section 4.3, it is shown that a number of security threats exist, which can compromise the security of a network resulting in illegal access to data. Also, a number of attacks are known to compromise the integrity of data. Protecting data, therefore, should be the end goal of every IT security measure (MIT, 2016).

In view of the advancement in IoT, data protection will become even more important. It is true that IoT generates a tremendous amount of data (Aazam *et al.*, 2014:414) due to its many connected devices. It is estimated that by the end of 2019 the amount of data produced by humans, machines, and things will be in the range 500 zettabytes (Ni *et al.*, 2018:601).

For instance, in a smart home, a large amount of data is generated from smart meters to smart thermostats, to the many sensors that may be connected in the home, and smart appliances. Most of this data are of no value, if it is not sent to server applications in the cloud where the data can be analysed to benefit the householder. Chapter 3 also highlighted some limitations which most IoT devices will have when it comes to resources such as memory, hence they cannot store a large amount of data. Therefore, IoT will greatly rely on cloud computing for the storage, processing,

and interpretation of its data. The data generated in a HAN will face many challenges. First of all, there is a high risk of data being stolen while it is transmitted between the HAN and the internet. Secondly data collected by the utility companies and device manufacturers will be stored online making it a target for cybercriminals.

How secure is data stored online? The slow adoption of cloud computing, especially by organizations, has always been around the issue of data security and privacy protection (Chen & Zhao, 2012:647) due to the insecure nature of the internet. In essence, storing data in the cloud means that the user has no control over it. In the current setup of things, service providers have been providing users with the assurance of their data through the use of a service level agreement (SLA) (Kandukuri *et al.*, 2009:517), but it is proven through research that cloud computing is not as safe as many service providers might claim (Chen & Zhao, 2012:647). According to Wang *et al.* (2010), cloud storage is not yet safe for sensitive data; this is mainly because cloud storage does not guarantee integrity and availability of data. With the establishment of bodies such as the cloud security alliance (CSA) and the use of security content automation protocol (SCAP) (Ali *et al.*, 2019:460), cloud security can see a significant improvement in data security. It will take time before everyone follows any standards set, as it was discussed before, the lack of standardisation in IoT is a significant problem. Ali *et al.* (2019:460) argue that large cloud vendors, such as Microsoft, Amazon, Google, and others, use proprietary technologies. This heterogeneity may result in security problems. Data security does not only involve storage but also protection during transmission as well.

4.2.4 IoT in context of network security

Network security is defined as a means to protect network services and equipment from modification or disclosure of transmitted information. While network security focuses on preventing illegal attacks, access to the network resources; data security focuses on keeping sensitive network data confidential (Yan *et al.*, 2015:293).

Despite the advancement in computer technology, 40 years down the line, the main goals of computer network security remains the same, that is to provide confidentiality, integrity, and availability (Fisch *et al.*, 2017). These three aspects are extended in order to provide security in a

HAN where confidentiality of data seems to be a concern with the introduction of smart technologies.

- I. *Confidentiality*: confidentiality involves giving access to data within a computer system or data that is transmitted between network devices, only to users with authorized access (Fisch *et al.*, 2017:2).
- II. *Integrity*: integrity stipulates that data in a computer system or data that is being transmitted between computers remain free of tampering, that may include any kind of modification to the data or fabrication of data (Fisch *et al.*, 2017:2).
- III. *Availability*: availability means when a user of a particular system requires access to the system, it must be available to service the request (Fisch *et al.*, 2017). In a networked environment, availability is crucial for a reliable running network. From time to time, a system may be rendered unavailable as a result of a Denial of Service (DoS) attack (Easttom II, 2019:9).
- IV. *Authorisation*: authorisation is to ensure that every access to resources is carried out by someone with the correct access rights (Ali *et al.*, 2017:2).
- V. *Authentication*: authentication verifies users in communication as to whom they claim to be (Ali *et al.*, 2017:2).

Before launching an attack, an intruder will need to gather information about the system or network he wants to target. The aim is to gather as much information about the targeted network as possible. Hoque *et al.* (2014:307) describe information gathering as an attempt by the attacker to gather enough vulnerability information about the network, which in turn will help the attacker be better informed as to how he/she can go about initiating the attack. Due to the nature of wireless networks when it comes to signal propagation, all that is required for an attacker to intercept the communication, is for him/her to be in the range of a wireless network (Anjum & Mouchtaris, 2007:9), and making use of equipment such as a laptop and network tools. Several network tools exist which can be used to gather information before an attack is launched. In this section, focus will be on some tools which can be used to gather information from targeted networks.

Network information-gathering tools come in different types based on the information one is trying to gather. The categories of information to be collected may include, services and port numbers they are running on, operating systems being used, types of devices connected to the network, protocols being used and so on (Hoque *et al.*, 2014:310).

4.2.4.1 *Packet sniffing tools*

Packet sniffing is the method of tapping each packet as it crosses the network. Packet sniffers are applications that are used to read data from packets as these packets travel across the network layer (Ansari *et al.*, 2002:17). The data in these packets can then be analysed and interpreted to get the information required. Many packet sniffing tools exist today. The majority of these however, are found on the Linux platform as open-source applications, thus it is easy for an attacker to obtain these.

Table 4-1 lists a few of these tools and their purposes.

Table 4-1 Network information gathering tools (Hoque et al., 2014:310)

Tools	Purpose	Source
Wireshark	Packet capturing	https://www.wireshark.org/
Tcpdump	Packet capturing	http://www.tcpdump.org/tcpdump_man.html
Angst	Sniffing	http://angst.sourceforge.net/angst.8.html
Ettcap	Man-In-The-Middle Attacks	https://ettercap.github.io/ettercap/
Tcptrace	Traffic Analysis	http://www.tcptrace.org/

4.2.4.2 *Network scanning tools*

Network scanning tools are used to scan an entire network and generate a report about network hosts, port being used etc. (Hoque *et al.*, 2014:311). The data collected may provide an attacker with enough information about vulnerabilities that may exist on the network, allowing him/her to launch an attack in return. For instance, before an attacker would launch an attack, he/she would

use software such as Nmap. According to Specht and Lee (2004:5), Nmap will allow the attacker to select ranges of IP addresses. In turn, for each scanned IP address, the tool will be able to gather port types and number being used, even the version of the OS in use.

Table 4-2 Network scanning tools adapted from Hoque et al. (2014)

Network scanning tools	Purpose	Source
Nmap	Scanning	https://nmap.org/
Wireshark	traffic scanning	https://www.wireshark.org/
Unicornscan	Scanning	http://sectools.org/tool/unicornscan/
Ike-scan	Host discovery	http://sectools.org/tool/ike-scan/

Chapter 3 gave an overview of the types of protocols used in a LAN, WLAN, and IoT based networks. A typical smart home may have all these networks working together. Thus the, tools discussed here should be able to work in a HAN. There exist several information-gathering tools designed specifically for networks using low energy protocols, such as ZigBee. An example of this is Wisens; which is a wireless network sniffer/analyser tool, designed to work on IEEE 802.15.4 PHY/MAC radio signals (Zhao *et al.*, 2012:538).

Due to the lack of hardware resources by most sensor-based devices, it becomes difficult to visualize what is going on in the network. SNAMP is a network scanning tool for WSN which is able to generate a topology of the network, analyse data generated by the sensors, report about the performance of the network and more (Yang *et al.*, 2006:1).

4.3 SECURITY VULNERABILITIES, THREATS, AND ATTACKS

In order to understand security as a whole, it is important to analyse the reasons why such security is vital, especially in a HAN, by reflecting the vulnerabilities, threats, and attacks to which such a network can be susceptible.

The architecture model of Vijayalakshmi and Arockiam (2016:34) was presented in Chapter 3, Section 3.8. This model presented in Figure 4-2 provides a visual representation of IoT architecture which is further applied in this section to IOT network security.

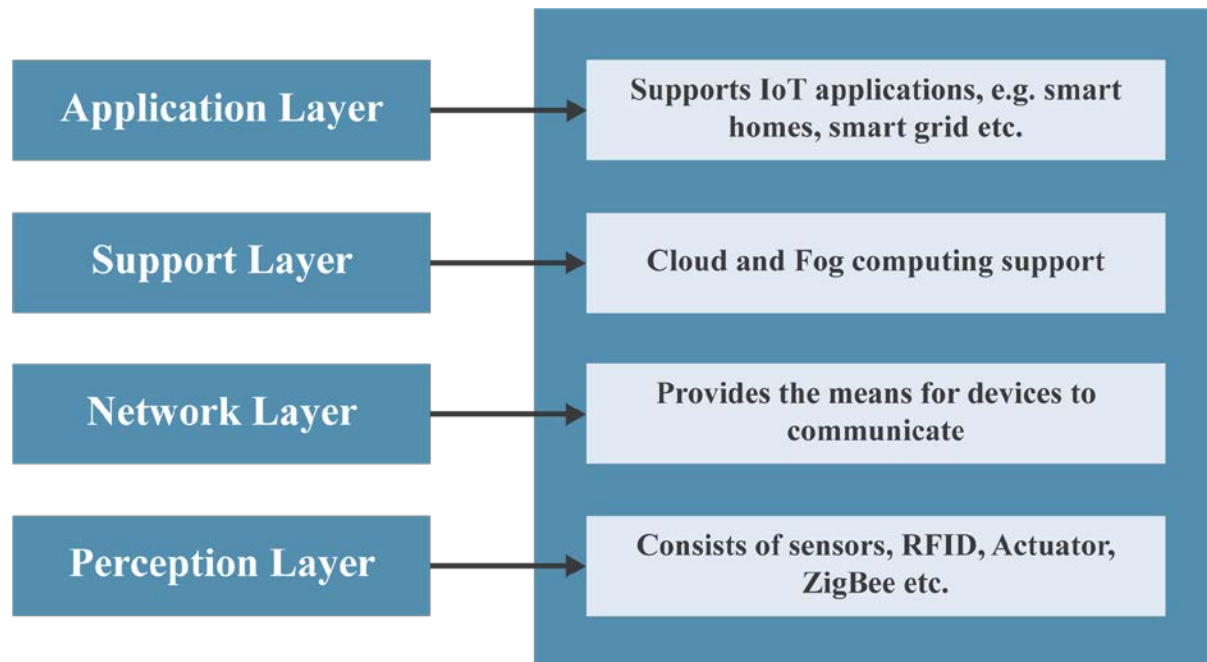


Figure 4-2 IoT architecture, adapted from (Ali et al., 2019)

4.3.1 IoT security vulnerabilities

The previous chapter concluded with a list of vulnerabilities intuitively compiled from the discussion of the components of an IoT. These aspects frequently appear in literature on IoT security. A discussion is presented here of the vulnerabilities based on literature on IoT security.

Experts believe that IoT networks are extremely vulnerable to attacks due to the following facts, (1) the unattended nature of most IoT devices; (2) most communications in IoT are wireless, making eavesdropping easy; (3) the low capabilities of IoT devices in both power and hardware, makes it difficult to implement strong security measures (Atzori *et al.*, 2010:2801). According to Ali *et al.* (2019:1), resource-constrained IoT devices makes it difficult to implement traditional security mechanisms such as cryptography, exposing these devices to data integrity and

confidentiality issues. In addition, Zhang and Zhu (2011:511) describe hidden dangers to information security in IoT. Such as the wide application of RFID tags, and the way information is processed and stored. Taking into consideration the risks which IoT possess, it is necessary that measures be implemented to protect the privacy of users in HANs. Lack of privacy has been the root cause of most concerns expressed alongside IoT. Atzori *et al.* (2010) acknowledges that “IoT represents an environment in which the privacy of individuals is utterly jeopardized in various ways”.

Weber (2010b:24) describes privacy as “the concealment of personal information as well as the ability to control what happens with this information”. It is a fact that the power of objects in IoT will be their ability to change the state of the environment and the generation of data (Gartner, 2014). This generated data is collected, the amount of connected IoT devices, such as smart appliances, smart meters and many more. For instance, through its security policy, Samsung acknowledges collecting data through its smart TVs. Privacy, therefore, should ensure that individuals have control over what data is being collected, for what purpose, who is collecting the data, and for how long is the data going to be stored.

Sathu and Shukla (2007:87) have also concluded that smart homes will have significant security challenges due to the lack of security knowledge by most of these households. For instance, most users operate in the administrator account on their PCs, password control is always feeble, computers are sometimes left on the whole night connected to the internet, and there are no backups done regularly or at all. These poor security practices can also be brought into IoT networks, resulting in real security challenges for smart homes where most smart appliances will have no ability to detect malicious infections.

In a survey done by Canonical (2017:5), it was discovered that a number of factors contribute to vulnerabilities in IoT devices today, these factors include:

- *Hard-coded passwords*: they argue that the majority of IoT devices are shipped with no password or the standard admin password which is known and exploitable;
- *Fundamentally weak security at both the software and hardware levels*: they argue that many IoT devices are not designed with security best-practice as a priority;

- *Lack of software updates:* the survey argues that when a vulnerability is found, manufacturers are not quick to roll out updates in time, or it might happen that no updates are released at all;
- *The size of the opportunity:* the billions of IoT devices which have been sold in the past few years mean the attack surface has also increased tremendously. This poses a high risk for attacks such as DDoS. As these devices become more integrated into the industry and society at large, the survey argues that organised attacks will also increase.

Canonical (2017:6) blames these vulnerabilities on a number of issues, among them, poor product design by manufacturers, lack of regulation, and the fact that no one is taking ownership of the security problems which exist. The table used to summaries intuitively understood vulnerabilities may now be updated and substantiated from this information. The updated table is provided in the final section of this chapter to provide guidance to the empirical study.

4.3.2 IoT network security Threats

It has been argued in this chapter that connectivity in an IoT network contributes substantially to the risk in the smart home. Although the architecture module provided in Figure 4-2, presents networks a separate layer it is evident that it central to the operation of the system as a whole.

Network security threats can be explained according to Bhaskar (2008:24), under the following four categories: interruption, interception, modification, and fabrication.

- I. *Interruption:* in a network setup, most communication takes place between clients and servers. The communication between these clients and servers may be interrupted using various techniques resulting in the services being provided by the servers to be unavailable to clients (Bhaskar, 2008:24). A number of attacks exist that may cause interruption to a system, such as denial of service (DoS).
- II. *Interception:* in network communication, an attacker can make use of various tools, such as packet sniffers, to intercept traffic between the sender and the receiver, and be able to read the contents of the packets. This type of threat may result in a problem of confidentiality (Bhaskar, 2008:24). Interception is passive in nature, whereby the intention

of the attacker is to gain access to information by using methods such as eavesdropping, no tampering of data takes place.

- III. *Modification*: unlike interception which is passive, modification is active (Bishop, 2005:5). With modification, packets are captured, and the contents of these packets are altered before the packets are forwarded to the targeted recipient; this causes a problem of data integrity (Bhaskar, 2008:25). Modification can also be used by an attacker to alter data in a database, or even change the working of hardware by changing certain settings.
- IV. *Fabrication*: fabrication aims at corrupting the authenticity of the data (Bhaskar, 2008:25). With fabrication, an attacker will try to send a message to a recipient pretending to be who they are not, or the attacker might insert a record in a database without permission. (Bishop, 2005:5).

4.3.3 IoT security attacks

A network security attack can be any action that compromises the integrity of information in a network (Bhaskar, 2008:25). Silberschatz *et al.* (2018:642) define a security attack simply as “*the attempt to break security*”. Every network employs several security mechanisms to prevent attacks. The aim of an attacker may be to exploit any vulnerability that may exist in a network resulting in a threat (Hoque *et al.*, 2014:308), and when such threats are exploited, the outcome is an attack.

In this era of interconnection, more and more people depend on networked services for business, entertainment, or just any day to day activities (Schneider, 2012:15). According to Hoque *et al.* (2014:308), it is in these network services that attackers intentionally keep looking for loopholes by gathering necessary information that will allow them to launch an attack. Network attacks occur on a day to day basis. Attackers continue to use the same old methods to gain access to unsuspecting networks and devices. Most of these attacks succeed due to loopholes that are left as a result of poorly configured networks, bugs in software, and out of date firmware, or even due to an outdated operating system. Security attacks can come in any of these two forms, passive or active (Ali *et al.*, 2017:2).

- I. *Passive attacks* have one common purpose and that is the gathering of information, the content of the message itself is not altered in any way. An example of a passive attack is eavesdropping (Kavitha & Sridharan, 2010:36).

- II. *Active attacks*, on the other hand, have one goal in mind, and that is to destroy data in a network, thus disrupting the normal functioning of a network (Jawandhiya *et al.*, 2010:4064). The attack may also involve packets being modified, or packets being injected into the data stream (Anjum & Mouchtaris, 2007:7).

Network attacks can originate from two sources, either internal or external to the network. It has been established that 70% of network attacks originate from within the network itself (Garzia, 2013:293), these are mainly from compromised hosts. A survey conducted by Hewlett-Packard (HP, 2014), revealed that 7 out of 10 attacks originated within the network itself from computers infected with malware.

In the section the layered architecture presented in Figure 4-2 are used to discuss security attacks in IoT networks.

4.3.3.1 Types of attacks based on the application layer

Due to a lack of standard in IoT application building, each application may employ a different security strategy, but one thing all applications have in common, is data sharing (Ali *et al.*, 2019). IoT devices are known to generate a tremendous amount of data, some of this data is shared among IoT devices themselves, but the majority end up in the cloud (Ni *et al.*, 2018:601). This section looks at security attacks that attackers use on this layer.

- I. *DoS attack*: applications are also prone to DoS attacks. An intruder can use DoS attacks to destroy the availability of the application or the service it provides (Frustaci *et al.*, 2018:2484).
- II. *Code injection*: with this type of attack, an intruder may inject malicious programming code into an IoT application, allowing him to exploit any vulnerabilities that the application may have (Frustaci *et al.*, 2018:2484).
- III. *Malware attacks*: an intruder can target IoT application with malware, such as trojan horse or worms to steal data from the device (Ali *et al.*, 2019:462).

4.3.3.2 Types of attacks based on the support layer

The support layer plays a vital role when it comes to storage of IoT data. Due to their lack in processing power, IoT devices collect data and send it to servers in the cloud for analysis, and the

results of such analysis may be sent back to the device so that it may take a certain action. Security attacks on this layer are aimed at either stealing data or modifying it. Let us look at various security attacks which may take place on this level.

- I. *Data security*: for data to remain secure in the cloud, it needs to be kept safe from security breaches (Ali et al., 2019:460). Among these breaches are a breach of integrity, confidentiality, and availability (Silberschatz et al., 2018:642).
- II. *Virtualisation security*: different cloud vendors make use of a variety of virtualisation technologies, some of these are known to bypass network security measures. (Ali et al., 2019:460).
- III. *Tenant's security*: clouds vendors host files from multiple users. A single storage volume might contain files from other users. If security is not well implemented on these file servers, one user can steal data from another (Ali et al., 2019:460).

4.3.3.3 ***Types of attacks based on the network layer***

Inheriting the challenges of wireless communication, IoT networks face its own challenges. In this section, we look at attacks which aim at network communication in IoT.

- I. *Denial of Service (DoS) and Distributed DoS (DDoS)*: Stewart et al. (2012:190) describe a DoS attack as “ a resource consumption attack that has a primary goal of preventing legitimate activity on a victimised system”. The attacker can overload the network with traffic above its capacity making the network unavailable in the process (Ali et al., 2019:460).
- II. *Eavesdropping*: eavesdropping attacks are known to be passive in their nature. An intruder can simply listen to the traffic for the purpose of duplicating it (Stewart et al., 2012:192). According to (Dai et al., 2013:1), attackers might use eavesdropping as a forerunner to a real attack, by gathering information about the targeted network. In wired network, it might require that an intruder get physical access to the network through an unused port in order for him to listen to the traffic. Wireless networks on the other hand, make the work of an intruder much easier. According to Anjum and Mouchtaris (2007:11), due to the nature of wireless networks, all an intruder will need is a suitable transceiver and being in the range

of the transmitted signal for him to be able to decode the transmitted message. Similar to other wireless technology, IoT relies heavily on wireless communication technologies.

- III. *Routing attacks*: Routing attacks simply target the routing protocol being used by the router, or it targets the routing table (Anjum & Mouchtaris, 2007:10). Its aim is to modify the right routing path during the collection and forwarding process (Frustaci *et al.*, 2018:2484).
- IV. *Sybil Attacks*: a Sybil attack involves a node assuming multiple identities (Anjum & Mouchtaris, 2007:118), by impersonating other nodes or claiming a false identity. One problem resulting from such an attack is when a malicious node claims multiple identities, the result is resource depletion on a system (Xiao *et al.*, 2009:492). This attack can also result in the distribution of fake routing information (Ali *et al.*, 2019:460).
- V. *Replay attacks*: a replay attack involves capturing data being transmitted from one destination to another, and using this captured data to perform unauthorized actions (Bhaskar, 2008:26). Replay attacks can be very dangerous to a smart home, where commands are sent from the HAN to control a number of smart appliances. An attacker can use a replay attack to cause havoc in the victim's home, thus disrupting normal functionality of smart appliances (Namboodiri *et al.*, 2014:514).

4.3.3.4 *Types of attacks based on the perception layer*

The perception layer describes all the IoT hardware and this section looks at some of the attacks relating to this layer.

- I. *Sleep deprivation attacks*: IoT devices are known to have limited power source due to their reliance on battery (Miorandi *et al.*, 2012:1502). The attack causes the sensor node to stay awake draining the battery in the process (Khan & Salah, 2018:399).
- II. *Malicious code injection*: this type of attack aims at compromising an IoT node by inserting malicious code into the node giving the intruder illegal access to the system (Ali *et al.*, 2019:460).

- III. *RFID spoofing*: this type of attack targets RFID-enabled nodes by spoofing the signal and stealing the RFID tag. Once the tag is known, the attacker can send fake data using the original RFID tag, gaining full access to a system as a result (Ali *et al.*, 2019:460).
- IV. *Physical attacks*: an example of this is node tampering where an intruder might cause damage to items such as sensors, or by replacing a node or part of its hardware (Frustaci *et al.*, 2018:2484).

Before these vulnerabilities, threats and attacks are summarised in Section 4.5 to use as guide for the empirical investigation, cryptography is discussed as method to protect data.

4.4 DATA PROTECTION: CRYPTOGRAPHY

Data protection, as indicated on Figure 4-1, in Section 4.2, is central to computer security. Methods to secure data by means of cryptography have been around since the inception of computer networks. These methods are designed to maintain data integrity and to prevent unauthorised access. The methods presented in this section is used to protect data during transmission (in motion) and while it is stored (in rest). Cryptography provides an extra layer of security to data during processing, transmission or storage (Stewart *et al.*, 2012:362). Today, symmetric algorithms such as advanced encryption standard (AES), and asymmetric algorithms such as Rivet Shamir Adelman (RSA) are widely used in computer systems (Ali *et al.*, 2019:462), resulting in integrity, confidentiality, authenticity, and non-repudiation of the data (Chandra *et al.*, 2014:83).

The word cryptography comes from the Greek word *crypto* (*kryptos*), which means secret or hidden, and the word *graphein* or *grapho* which means to write (Dictionary.com, 2019). Hence Luciano and Prichett (1987:1) were able to describe cryptography as the art and science of making communication incomprehensible except to the intended recipient. Whereas cryptography provides a broader outlook of how cryptographic systems operate, it is encryption which provides the process of hiding the information to make it unreadable (Zotos & Litke, 2005:1)

Cryptography has a long history dating back all the way to the time of Julius Caesar. It is believed that around 50 B.C, Caesar devised a method of hiding text when he sent messages to Marcus Cicero in Rome (Luciano & Prichett, 1987:2). The technique involved shifting the alphabets two

steps to the right. For instance, A becomes C, B becomes D and so forth. This cryptographic system came to be known as the Caesar cypher (Stewart *et al.*, 2012:362).

By the 19th century, cryptography had reached a different level of complexity thanks to advanced mathematics. For instance, during World War II, the Germans made use of the enigma machine to create more complex substitution cyphers (Stewart *et al.*, 2012:364). Cryptography is a very simple concept. Chandra *et al.* (2014:83) explains, that for any cryptographic system to work you will need a plain text and a cypher text. The plain text is encrypted with a cryptographic algorithm to produce a cypher text. The cypher text is then transmitted to a recipient. Once received, the recipient will apply a specific algorithm to the cypher text in order to retrieve the plain text (Stewart *et al.*, 2012:366). Cryptography falls under two broad categories, asymmetric encryption and symmetric key encryption, in Section 4.4.2 these are discussed in more detail.

Cyphers are the core means for encrypting messages. Carter and Magoc (2007:1) define a cypher as “*a well-defined procedure that states how to hide each character from the original text in the encrypted text and how the recipient should decrypt the cypher text to read the original message*”. Stewart *et al.* (2012) shows that cyphers convert messages from plain text to cypher text based on the following three bases. (1) cyphers can operate on a bit basis; (2) it can operate on a character basis, and (3) cyphers can operate on a block basis. A number of cyphers exist today, but there are two classical cyphers namely, substitution and the transposition cyphers (Uddin & Youssef, 2006:677), which form the basis for many encryption standards in use today (Carter & Magoc, 2007:1).

The discussion on cryptography starts with a description of the mechanics thereof in terms of classical cyphers.

4.4.1 Classical cyphers

Since the understanding of modern cyphers requires basic methods developed for classical cyphers, this discussion includes examples and discussion of methods developed during the evolution of cryptography. Classical cyphers may be categorised as substitution and transposition cyphers.

4.4.1.1 Substitution cyphers

Substitution cyphers simply replace one character with another one or a bit of the plaintext message with another one, explains Stewart *et al.* (2012:375). The Caesar cypher mentioned earlier is the simplest example of a substitution cypher (Carter & Magoc, 2007:2). Substitution cyphers also fall under two categories, mono-alphabetic and polyalphabetic (Mao, 2003:255-256).

Mono-alphabetic

The Caesar cypher, as shown in Figure 4-3, shifts three positions to the right to create a cyphered character, but the problem is that it runs out of characters. To fix this, the characters are wrapped around so that A becomes X, B becomes Y, and C becomes Z. To illustrate this, let P be the plaintext, C be the cypher text, and let K be the key.

Plain text, C be the cypher text, and let K be the key.

P =	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K =	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Figure 4-3 Caesar cypher (Luciano & Prichett, 1987:2)

Stewart *et al.* (2012:376) shows that by converting each letter to a decimal equivalent, such that A becomes 0 and Z becomes 25, it will be possible to express Caesar cypher in mathematical terms as shown in Figure 4-4. In such a way, C and P can be expressed as functions, whereby

$C = (P + 3) \bmod 26$ - represents the encryption function

$P = (C - 3) \bmod 26$ – represents the decryption function

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 4-4 Caser cypher in decimal representation (Luciano & Prichett, 1987:2)

For example, the word, “THE” becomes “WKH” since the decimal equivalent of each letter is used in the formula as follows:

$$C(T) = (19 + 3) \bmod 26 = 22 = W$$

$$C(H) = (7 + 3) \bmod 26 = 10 = K$$

$$C(E) = (4 + 3) \bmod 26 = 7 = H$$

While mono-alphabetic cyphers operate on a single character to hide the message, polyalphabetic cyphers make use of multiple characters within the same message (Stewart *et al.*, 2012:376).

Poly-alphabetic

Carter and Magoc (2007:3) describe a poly-alphabetic cypher as “simply multiple mono-alphabetic cyphers being applied to the same message”. A well-known polyalphabetic cypher is the Vigenère cypher, created by the French cryptographer bearing the same name (Luciano & Prichett, 1987:5). Kester (2013:142) describes this cypher as a series of Caesar cyphers based on the letter of a keyword. To better understand the working principles of this cypher, Stewart *et al.* (2012:377) gives a recipe which is easy to understand.

To encrypt a text, a key should be provided first. In our example, we will make use of “eagle” as the key. The steps for encrypting will be as follows:

1. Write out the plain text that needs to be encrypted.
2. Underneath each character of the plain text, write down the key repeating it as many times as possible to check again the whole text.
3. Convert each character position from plain to cypher text
 - a. First, locate the column header of the character in the plain text
 - b. Second, locate the row header with the corresponding character in the key
 - c. Then the encrypted character will be at the intersection of the column and row.
4. Steps 1 to 3 should be repeated for each character to be encrypted.

For instance, if the message to be transmitted was, everyone must take cover, making use of the Vigenère square in Table 4-3, the encryption process will look as follow:

Plain text:	e	v	e	r	Y	O	n	e	M	u	s	T	t	a	k	e	c	o	v	E	R
Key:	e	a	g	l	E	E	a	g	L	e	e	A	g	l	e	e	a	g	l	E	a
Cyphertext:	i	v	k	c	C	S	n	k	X	y	w	T	z	l	o	I	c	u	g	I	v

Table 4-3 Vigenère square (Kester, 2013:142)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	A	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

The Vigenère cypher can also be represented mathematically using modular arithmetic (Kester, 2013:142). The first step is to transform the letters of the alphabet into numbers whereby A=0 and Z=25. Thus, the encryption of a letter, such as X, can be expressed mathematically by applying a shift factor of n and mod 26, where 26 represents the number of characters in the alphabet. Hence the encryption function can be expressed as $\text{Enc}(X) = (x+n) \bmod 26$, and the decryption function can be written as $\text{Dec}(X) = (x-n) \bmod 26$.

The cypher can also be expressed alphabetically if we exchange the numbers 0 – 25 with the alphabets A - Z, and applying the encryption key K. The Vigenère encryption function E can be written in this manner:

$$C_i = \text{EK}(M_i) = (M_i + K_i) \bmod 26$$

and the decryption function D using the key K can be written as

$$M_i = \text{DK}(C_i) = (C_i - K_i) \bmod 26$$

whereby $M = M_0 - M_n$ represents the message, $C = C_0 - C_i$ represents the cypher text, and $K = K_0 - K_m$ represents the key used.

An extended version of this algorithm makes use of 92 characters instead of the common 26 characters of the greek alphabet. With this modified Vigenère cypher, the encryption and decryption functions are as written as follow:

$$\text{Encryption} - C_i = \text{EK}(P_i) = (P_i + K_i) \bmod 92,$$

$$\text{Decryption} - P_i = \text{DK}(C_i) = (C_i - K_i) \bmod 92$$

4.4.1.2 **Transposition cyphers**

A transposition cypher, as highlighted by Carter and Magoc (2007:3), produces a cypher text with the same symbols as the plain text when an encryption algorithm is applied to the plain text. The major difference with substitution is that only the position of the letters change and not the letters themselves (Kester, 2013:143). Transposition though becomes more efficient when a keyword is used to perform a columnar transposition (Stewart *et al.*, 2012:375).

The process provided by Kester (2013:143), will help us to have a better idea on the working principles of this cypher.

The steps are as follows:

1. Select a fixed-length key.
2. Write the plain text row by row in a rectangular form, but with a fixed column which is equal to the selected key.
3. Rearrange the columns into the alphabetical column using the key as the determinant.
4. Read the message column by column to generate the cyphered text.

When these steps are applied to an example, for instance, if the message “the eagle has landed, take your position” was to be encrypted. For this example, PROTECT will be used as the key.

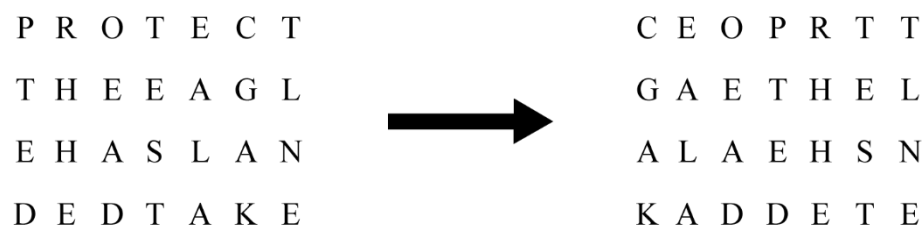


Figure 4-5 An example of columnar transposition

The cypher text will now be: “gakoxalapneaduitedyihheotestrolnesx”

4.4.2 Modern cryptography

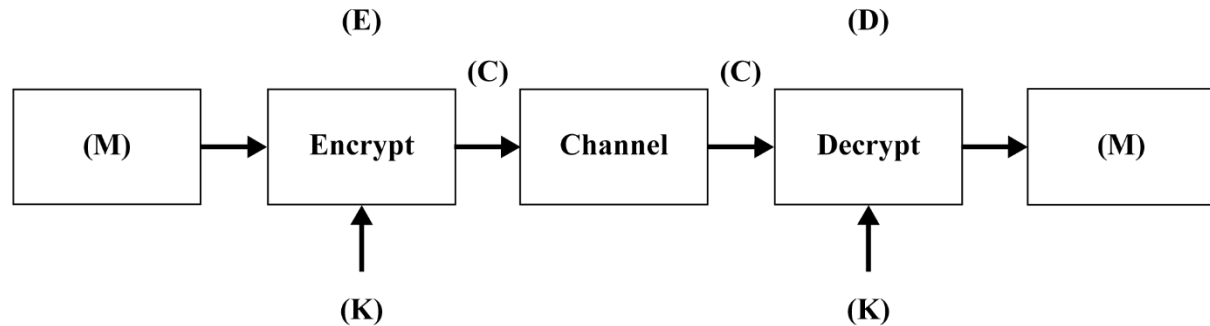
Some classic cyphers which was discussed in the previous section involve hiding the inner workings of the algorithm to others (Stewart *et al.*, 2012:381). The sender and receiver only knew the algorithm for encrypting and decrypting. Using this process, the security for the algorithm was insured. With modern cryptographic systems, though, the secret value is the key, and this is what is protected from attackers (Anjum & Mouchtaris, 2007:18).

Modern cryptography systems no longer hide the algorithms being used, in fact, Stewart *et al.* (2012:381) shows that most of the encryption algorithms are widely available to the public, such

as over the internet. Under modern cryptography, two categories exist, namely symmetric and asymmetric key cryptography.

4.4.2.1 *Symmetric key cryptography*

Symmetric key cryptography, also referred to at times as secret-key or shared key cryptography,



is a cryptographic system that utilises one key to encrypt and decrypt the information being transmitted (Chandra *et al.*, 2014). In essence, both the sender and receiver use the same key.

Figure 4-6 Basic operation of a symmetric key cryptography quoted from Anjum & Mouchtaris (2007:20).

Symmetric encryption can be expressed using the following notations where:

M: represents a plaintext message

C: represents cypher text

E: represents an encryption algorithm

D: represents a decryption algorithm

K: represents a set of keys

K_e : represents private key

K_d : represents a public key

By using the diagram in Figure 4-6, the encryption process can be explained as follows, the plaintext M is encrypted with the encryption algorithm E , using the encryption key K to generate the cypher text. The cypher text can then be transmitted wirelessly or using cables to its destination. Upon receipt, the decryption algorithm D is applied, using the decryption key K to retrieve the plaintext. Symmetric key cryptography is referred to at times, as private key cryptography, or

secret-key cryptography. Symmetric key algorithms fall into two categories block cyphers and stream cyphers.

Block cyphers: block cyphers work on a piece or block of a message and applying the encryption to the message one block at a time (Stewart *et al.*, 2012:381). Transposition and substitution cyphers fall under this category.

Stream cyphers: stream cyphers operate on each bit or byte of a message (Anjum & Mouchtaris, 2007:21). The majority of stream cyphers are known to be proprietary. Since stream cyphers operate on bits or bytes, they are known to be much faster than block cyphers.

4.4.2.2 *Asymmetric key cryptography*

In asymmetric key cryptography, a set of two keys is used for encryption and decryption as shown in

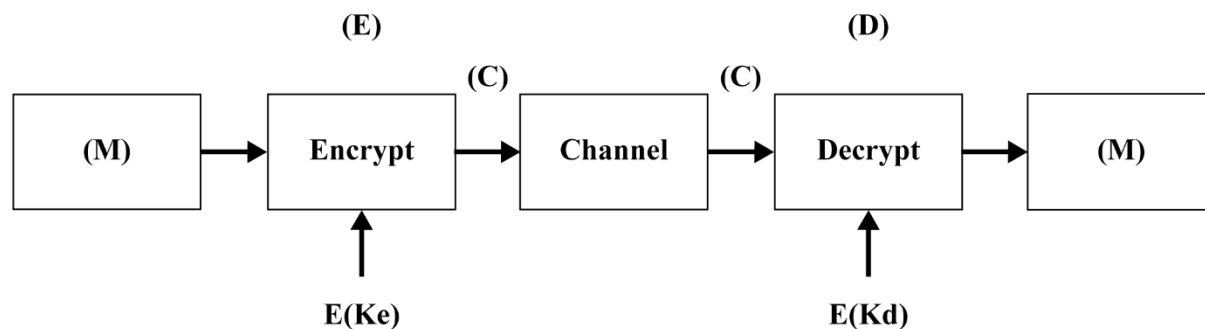


Figure 4-7 Asymmetric key cryptography quoted from (Stewart et al., 2012:406)

The public key is made available to anyone, while the private key is only known by the individual creating the message (Anjum & Mouchtaris, 2007:23). When the sender wants to transmit a message, he will use the public key of the receiver to encrypt the message. The receiver will then use his private key to decrypt the message (Chandra et al., 2014:84).

The strength of asymmetric cryptography lies in the fact that the encryption algorithm is made available for public scrutiny, making the choice of keys the only basis for its strength (Mao, 2003:294). In symmetric cryptography where one key is shared among the parties communicating, getting hold of this key would put the communication in danger. With asymmetric cryptography, though, even if one person knows the public key, it is impossible to derive the private key from

the ciphered text (Stewart *et al.*, 2012:405). Another problem that symmetric cryptography suffers from is the inability to prove if the sender of the message is who he claims to be. Asymmetric cryptography uses the private key to sign a message, thus ensuring non-repudiation (Anjum & Mouchtaris, 2007:24). For instance, a written letter can be confirmed to come from the sender by checking his signature. In the same way, asymmetric cryptography provides the means to sign a message digitally. The private key is used to create the signature; then the public key is used to verify it.

4.4.2.3 Examples of symmetric and asymmetric cryptography algorithms

Some algorithms exist under symmetric and asymmetric cryptography systems, namely Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) algorithms.

Advanced Encryption Standard (AES)

In September of 1997, a decision was taken by the National Institute of Standards and Technology (NIST) for a new encryption standard (Lu & Tseng, 2002:1). By the year 2001, AES was introduced by the National Institute of Standards and Technology to replace the aging DES standard (Harrison & Waldron, 2007:215).

AES is asymmetric, block-based cypher encryption standard (Abbasi & Younis, 2007:2). As a block cypher, AES processes data into blocks of 128 bits (Hamalainen *et al.*, 2006:2), the Rijndael version of AES though, extends the length of these blocks to be the same size as the keys. These keys sizes are 128, 192, and 256 bits (Stewart *et al.*, 2012:391). To help with the understanding of AES operation, the 128-bit version of AES will be the focus of this section.

AES operates on data in four groups of four bytes known as a state (Anjum & Mouchtaris, 2007:23). A state is merely an internal representation of information in a four by four matrix of bytes (Hamalainen *et al.*, 2006:2). According to Bhaskar (2008:85), a state can also be represented as an array of columns, where each column in the array accounts for a single byte, and the array has four rows. Hamalainen *et al.* (2006:2) show that each state is filled with data coming from the result of the data that has been XORed with the cypher key.

Each state then goes through some transformations namely, AddRoundKey, SubBytes, ShiftRows, MixColumns, and KeyExpansion (Lu & Tseng, 2002:2) to produce an output. In addition to these

transformation steps, each state will loop through these five steps a number of times known as the conversion round (Nr) as shown in Table 4-4 Number of transformation round (No) vs. Block length (Bhaskar, 2008:85)Table 4-4. The table indicates that for a different key size and data block size, the number of transformation rounds will be different.

Table 4-4 Number of transformation round (No) vs. Block length (Bhaskar, 2008:85)

	Round No	Block size		
		128 bits Nb=4	192 bits Nb=6	256 bits Nb=8
Key Size	128 bits Nk=4	10	12	14
	192 bits Nk=6	12	12	14
	256 bits Nk=8	14	14	14

To better understand how No integrates with the five transformation states, Lu *et al.* (2010:2) explain the AES encryption and decryption processes as functions using the following notation:

Table 4-5 AES encryption and decryption algorithms (Lu & Tseng, 2002:2)

AES Encryption	AES Decryption
AddRoundKey for round=1 to Nr-1 SubBytes ShiftRows MixColumns AddRoundKey end for SubBytes ShiftRows AddRoundKey	InvAddRoundKey for round=1 to Nr-1 InvSubBytes InvShiftRows InvMixColumns InvAddRoundKey end for InvSubBytes InvShiftRows InvAddRoundKey

In Table 4-5, the five transformation steps are expressed as functions. The for-loop presents the number of rounds.

Rivest Shamir Adleman (RSA)

RSA is a block cypher based on asymmetric cryptography, meaning that it relies on two sets of keys, a public key, and a private key. Since its release in 1978 (Aboud *et al.*, 2008:127), RSA has had many applications, such as in hardware (Brickell, 1989:1; Fournaris & Koufopavlou, 2005:4645-4648); in handshake protocols such as SSL and TSL (Jonsson & Kaliski Jr, 2002:127-141); in cloud computing (Somani *et al.*, 2010:211-216); and also as a digital signature (Somani *et al.*, 2010:214) to prevent non-repudiation. Today, some major IT companies, such as Microsoft, Cisco, and Nokia, security solutions rely heavily on RSA (Stewart *et al.*, 2012:406).

According to the Request For Comment (RFC) 2313 document on RSA encryption (Kaliski, 1998:8), RSA encryption process comprises of four steps, namely encryption block formatting, octet-string-to-integer conversion, RSA computation, and integer-to-octet-string conversion. An RFC document contains technical and organizational notes about the internet. These notes vary from computer networks to protocols, procedures, and concepts (ETF, 2017). RSA security depends mainly on the difficulty to factor large prime numbers (Bhaskar, 2008:92). RSA algorithm according to Stewart *et al.* (2012:406) and Mao (2003:308), is described in the following steps:

1. Choose two random prime numbers p and q
2. Compute the product of the two number, such that $n=p*q$
3. Select a number e such that,
 - a. $e < n$
 - b. e and $(n-1) (q-1)$ are prime
4. Find a number, d , such that $(ed - 1) \bmod (p-1) (q-1) = 0$
5. Distribute e and n as the public key to all that need to use it. Keep d secret as the private key.

Using p and q , two users are now be able to communicate securely. For instance, if Kaja and Clarisse wanted to communicate, assuming Kaja has the private key, and Clarisse has her public key. To send a private message P to Kaja, Clarisse will have to generate a cypher text C , using the following formula (where e is Kaja's public key, and n is the product of p and q):

$$C = P_e \bmod n$$

When Clarisse receives the encrypted message, she will use the following formula to decipher the message:

$$P = C_d \bmod n.$$

4.4.3 Cryptography and network protocols

The purpose of cryptography is to provide confidentiality, authentication, message integrity, and non-repudiation. Some network protocols that exist today have incorporated cryptography into their functionality. For instance, IPsec is a suite of protocol that was designed to provide end-to-end encryption between sender and receiver. IPsec consists of two protocols, the authentication header protocol (AH) which provides message authentication, integrity, and anti-replay of messages (Bishop, 2005:162). The other protocol is the encapsulating security payload (ESP), which provide confidentiality, but can also provide some functionalities provided by AH (Ferguson & Schneier, 2000:7).

Some application layer protocols also have any equivalent secure version of its protocol. For instance, HTTP has HTTPS used by web servers, FTP has FTPS, and email servers rely on SSL and TLS. There exist some protocols that do not have a secure version, such as DHCP, and for these, IPsec will be a better alternative.

Due to the vulnerability of wireless networks, encryption was necessary (Buttyán & Dóra, 2006:2). Hence today we find different protocol being used on Wi-Fi networks, these include Wired Equivalent Protocol (WEP), and Wi-Fi Protected Access (WPA). WEP makes use of a predetermined key to encrypt data before it leaves the network. It supports the key length of 64-bits, 128-bits, and 256-bits long (Reid, 2008:253). WEP was designed to provide security for Wi-Fi networks, but it was not able to do that because its design was flawed from the start. Buttyán and Dóra (2006:5-6) discuss some of these design flaws in connection with authentication, integrity, and confidentiality. It did not take long before cryptanalysts found their way around WEP, as shown by Rowan (2010:10), it would take 5 to 30 minutes, depending on the strength of the signal, to crack a WEP key.

To overcome some of the design flaws of WEP, WPA was introduced. The major difference between the two was the way keys were generated. WPA introduced a new key management

scheme known as the temporal key integrity protocol (TKIP) (Rowan, 2010:10). What this entailed was that, instead of using the same key as in WEP, with WPA a new key was generated dynamically every time a client connected to the access point (Reid, 2008:256).

Despite the improvement in encryption, wireless networks remain vulnerable to attacks. Therefore, for wireless networks, security needs to be implemented at different levels. Hence the layered approach to wireless security. Measures such as changing the default password of the router, disabling SSID broadcasting, firmware upgrades and, MAC address filtering. These are just a few measures which contribute to a safer Wi-Fi network.

4.4.4 Current cryptographic solutions in IoT and their limitations

Unfortunately the traditional encryption methods discussed in Section 4.4.1 require more CPU power and consume more power (Ali *et al.*, 2019:462). The majority of IoT devices are characterized by low capabilities in terms of both power and resources; this will limit the level of security that can be implemented in such devices (Atzori *et al.*, 2010:2801). Ali *et al.* (2019:462) concludes that it is important to modify the current encryption algorithms or to create new ones for battery-operated IoT devices. It is true that encryption is one of the effective mechanisms for achieving data security in IoT, but it cannot work in isolation. According to Canonical (2017:10), even in places where encryption is deployed, it alone can't guarantee device protection or data privacy. In worse case scenarios, encryption would be rendered useless if an intruder gains physical access to a device.

To achieve total security in IoT, security will need to be implemented at different levels, such as data protection, physical device protection, network protection, and operating system protection. When it comes to network protection, various IoT protocols have been designed with security in mind. For instance, a protocol such as ZigBee, which is based on IEEE802.15.4 standard, implements a level of encryption (Zigbee.org, 2019). The IEEE 802.15.4 standard was designed to provide the basis to build protocols for IoT devices, which are secure and energy-efficient. It makes use of the AES encryption algorithm, with a 128bit key (Liberium, 2016).

Canonical (2017:16) does not believe the solution to security in IoT lies solely with encryption. With their Ubuntu Core OS, which was designed for IoT devices with security in mind. It claims that Ubuntu Core OS “*will take the burden of IoT security away from manufacturers, designer,*

and most importantly end user”. IoT security remains a very active topic of interest among researchers globally today (Ali *et al.*, 2019). As the technology matures, better security measures will be developed and implemented, but as things are currently, IoT, especially with view to smart homes, it still has serious security challenges (Ali *et al.*, 2017:1)

4.5 SUMMARY OF IOT SECURITY TO CONSIDER IN EMPIRICAL INVESTIGATION

In order to guide the empirical investigation of the study, the current and previous chapter are summarised in terms of security aspects identified from literature. Table 4-6 Updated security aspect based on IoT network architecture Table 4-6 provides an updated version of the list compiled in Chapter 3, Section 3.8, from this literature investigation into IoT network security.

Table 4-6 Updated security aspect based on IoT network architecture

Component	Security aspect
Application layer	
Appliance user interfaces (Section 3.2) (Sathu & Shukla, 2007:87)	Smart appliances have specific settings which can be manipulated by the user. This is inherently an advantage and a threat as described for gateways. Lack of password control.
Gateway user interfaces (Section 3.5) (Sathu & Shukla, 2007:87)	Again, a user interface creates opportunities for control of security settings but also vulnerabilities due to lack of knowledge by the user. Unauthorised access might be possible.
Mobile user interfaces (Atzori <i>et al.</i> , 2010:2801).	Mobile device applications pose many vulnerabilities to the home owner. The application programs to control the hub including the mobile application creates vulnerabilities since RFID can be simulated and other malicious command can be generated by potential attackers. Privacy is jeopardised.
<i>Application layer: Possible Attacks</i>	
• <i>DoS attack</i>: applications are also prone to DoS attacks. An intruder can use DoS attacks to destroy the availability of the application or the service it provides (Frustaci <i>et al.</i>, 2018:2484). • <i>Code injection</i>: with this type of attack, an intruder may inject malicious programming code into an IoT application, allowing him to exploit any vulnerabilities that the application may have (Frustaci <i>et al.</i>, 2018:2484). • <i>Malware attacks</i>: an intruder can target IoT application with malware, such as a Trojan horse or worms to steal data from the device (Ali <i>et al.</i>, 2019:462).	
Support Layer	

Component	Security aspect
Connection from gateway to cloud (Section 3.7) (Chen & Zhao, 2012:647)	Connection to the internet creates vulnerabilities.
Cloud service provider (Section 3.7) (Chen & Zhao, 2012:647).	Data storage by service provider also has vulnerabilities and might be subject to attacks.
<i>Support layer: Possible Attacks</i>	
• <i>Data security</i>: for data to remain secure in the cloud, it needs to be kept safe from security breaches (Ali <i>et al.</i>, 2019:460). Among these breaches are a breach of integrity, confidentiality, and availability (Silberschatz <i>et al.</i>, 2018:642). • <i>Virtualisation security</i>: different cloud vendors make use of a variety of virtualisation technologies, some of these are known to bypass network security measures. (Ali <i>et al.</i>, 2019:460) • <i>Tenant's security</i>: clouds vendors host files from multiple users. A single storage volume might contain files from other users. If security is not well implemented on these file servers, one user can steal data from another (Ali <i>et al.</i>, 2019:460).	
Network Layer	
Connection of sensors to Gateway (Sections 3.4 and 3.7) (Atzori <i>et al.</i> , 2010:2801).	Each sensor and its node use specific protocols to connect to the gateway. Wireless communication susceptible to eavesdropping.
Gateway Configuration (Section 3.5 and 3.7)	The ability of the user to manipulate security settings of gateways is both an advantage and vulnerability. It is an advantage when the user has enough knowledge of hardware, but when a user is not knowledgeable it becomes a vulnerability.
Gateway operating system (Sections 3.6 and 3.7)	The sophistication of the operating system used by the gateway creates specific vulnerabilities.
Gateway hardware capacity (Section 3.5 and 3.7)	Aspects such as processor power and memory capacity influence the ability of the gateway to implement security measures and encryption.
Gateway mobile connection (Section 3.5 and 3.7)	The connection between the mobile phone and the gateway has inherent network vulnerabilities.
General connectivity threats (Bhaskar, 2008:24)	Network security threats can be viewed in terms of the following four categories: interruption, interception, modification, and fabrication.
<i>Network layer: Possible Attacks</i>	
• <i>Denial of Service (DoS) and Distributed DoS (DDoS)</i>: Stewart <i>et al.</i> (2012:190) describe a DoS attack as “a resource consumption attack that has a primary goal of preventing legitimate activity on a victimised system”. The attacker can overload the network with traffic above its capacity making the network unavailable in the process (Ali <i>et al.</i>, 2019:460). • <i>Eavesdropping</i>: eavesdropping attacks are known to be passive in their nature. An intruder can simply listen to the traffic for the purpose of duplicating it (Stewart <i>et al.</i>, 2012:192). • <i>Routing attacks</i>: Routing attacks simply target the routing protocol being used by the router, or it targets the routing table (Anjum & Mouchtaris, 2007:10). Its aim is to modify the right routing path during the collection and forwarding process (Frustaci <i>et al.</i>, 2018:2484).	

Component	Security aspect
• <i>Sybil Attacks</i>: a Sybil attack involves a node assuming multiple identities (Anjum & Mouchtaris, 2007:118), by impersonating other nodes or claiming a false identity. • <i>Replay attacks</i>: a replay attack involves capturing data being transmitted from one destination to another, and using this captured data to perform unauthorized actions (Bhaskar, 2008:26).	
Perception layer	
Sensors	
Image sensors: Camera and video camera (Section 3.4)	Images and videos are potentially captured without the knowledge of the homeowner and stored on the device or transmitted to the cloud.
Sound sensor: microphone (Section 3.4)	Sound clips are recorded, and potentially can be duplicated for remote voice activation of control devices.
Temperature / light sensors (Section 3.4)	Environmental conditions can be manipulated to achieve specific outcomes.
RFID tags (Section 3.4.5) Zhang and Zhu (2011:511)	The tags of sensors can be simulated or duplicated to gain unauthorised access.
Sensor Nodes	
Nodes and small computers (Section 3.4.2) Canonical (2017:5)	Due to size and cost factors the hardware capabilities are insufficient to support traditional operation systems and network protocols, leaving these devices vulnerable to attacks.
Sensor node operating systems (Section 3.6)	The appliances and hubs are loaded with operating systems to control the hardware. Due to size and cost considerations these operation systems are not on the same standard as PC operating systems in terms of security considerations. These smaller operating systems are vulnerable to code attacks and memory errors which may be exploited.
Smart electricity management	Vulnerabilities caused by service providers knowing the consumption patterns of home owners.
Smart meters (Section 3.3)	Communication between smart meter and utility supplier could jeopardise the privacy of the homeowner in that the communication could identify when the homeowner is not at home.
<i>Perception Layer: Possible Attacks</i>	
• <i>Sleep deprivation attacks</i>: IoT devices are known to have limited power source due to their reliance on battery (Miorandi <i>et al.</i>, 2012:1502). The attack causes the sensor node to stay awake draining the battery in the process (Khan & Salah, 2018:399). • <i>Malicious code injection</i>: this type of attack aims at compromising an IoT node by inserting malicious code into the node giving the intruder illegal access to the system (Ali <i>et al.</i>, 2019:460). • <i>RFID spoofing</i>: this type of attack targets RFID-enabled nodes by spoofing the signal and stealing the RFID tag. Once the tag is known, the attacker can send fake data using the original RFID tag, gaining full access to a system as a result (Ali <i>et al.</i>, 2019:460). • <i>Physical attacks</i>: an example of this is node tampering where an intruder might cause damage to items such as sensors, or by replacing a node or part of its hardware (Frustaci <i>et al.</i>, 2018:2484).	

4.6 SUMMARY

The objective of this chapter is to review literature on network security in order to identify threats to homeowners and to guide the empirical study. This objective is achieved by first considering IoT security in the context of hardware, software, data, and network security.

It is argued in Section 4.2, that hardware, software and network security have the joint purpose of protecting data. In an IoT network this is very true. With so much data collected by sensors, it is the responsibility of the of the hardware, software and network designers to ensure that the data is protected.

In Section 4.3 various aspects of security were discussed, vulnerabilities, threats and attacks. It was found that vulnerabilities can be found in the hardware (in the form of firmware) or in software (such as mobile apps). Vulnerabilities may also exist due to poor network configuration of devices. Attackers may exploit these vulnerabilities, which may then lead to threat and attacks.

It was established (Section 4.4) that the role of computer security is to provide confidentiality, integrity, and authentication. Encryption has been used for years in computer networks to provide these security measures. Unfortunately, due to the limitation in processing power in many smart appliances and objects, performing encryption on these devices would be impossible. One solution is to modify current encryption algorithms to be compatible with IoT devices.

This chapter has demonstrated that the addition of smart objects into a HAN might expose users' privacy if certain security guidelines are not followed or implemented by the people setting up the network or even by device manufacturers. For instance, encryption and other security measures might have been built in some smart appliances and devices, but the lack of security knowledge of users in a HAN, may render these features useless. Thus, it rests upon device manufacturers to ensure that the security of these smart objects is plug and play the moment the device is connected to a network.

Some manuals that come with most appliances are sometimes difficult to understand by everyone. Hence it is vital that manufacturers educate home users, in layman's terms, the dangers involved if these guidelines are not followed. The manufacturers also should be transparent as what type of data they collect through these devices and for what purpose. The success of a smart home rests heavily on how users' privacy can be protected. It is true a smart home can make the lives of people

very convenient (Ali *et al.*, 2017), but they need to first of all trust these devices. Thus security concerns of smart objects remain one of the deciding factors by users trying to embrace the technology into their homes.

In Chapter 5, a number of documents concerning selected IoT devices and smart appliances are analysed to enhance understanding of the theoretical position of this study as summarised in Section 4.5.

CHAPTER 5 EMPIRICAL INVESTIGATION

5.1 INTRODUCTION

The main purpose of this study is to identify security threats posed by smart home devices to unsuspecting homeowners in relation to their privacy in a home area network.

The objective of this chapter is to fulfil the empirical objective of the study, by collecting data about security matters concerning smart appliances from manufacturers and reviewers. The data are analysed in order to identify possible security threats based on the literature on networks and security presented in Chapter 3 and Chapter 4 of this dissertation. The aim of this chapter is to provide an empirical investigation in support of the literature review in order to identify security concerns present in IoT networks.

It is the position of this study the majority of devices in an IoT network has similar architecture and that is mainly the perception layer that differs from appliance to appliance in terms of the sensors used to gather data. However as indicated in Chapter 3, the specific hardware configuration selected by a manufacturer has a major impact on the resulting security of a device. In the extreme the following scenario may exist: One smart TV may have sufficient memory and processing speed to support secure encryption of data managed by a secure operating system, while another smart TV has a poorly designed operating system with insufficient memory and does not encrypt data at all. This empirical investigation is aimed at discovering such detail in manufacturer's documents and reviewers' documents. The list of security concerns developed as conclusion for Chapter 4, guided the investigation.

This study is framed as interpretive and deductive in nature this implies that the aim of the empirical study is to reflect on the story told by the theory from the story told by the data. The aim is not to create a theory solely from the data as done in grounded theory studies. Data analysis is aimed at identifying threats from studying the selected data sources that are

not intuitive from the story told by the theory, as presented in Chapter 4. It is assumed the story told by the theory holds true for smart devices based on the components of these systems, the aim is to identify aspects of concern for the general home owner in terms of data management practices and specific components installed.

The chapter starts with a discussion of the research strategy applied in this chapter in Section 5.2. The aim of this section is to provide a roadmap for the rest of the chapter in terms of data collection, presentation and coding, and the development of guidelines as findings of the study.

This process is applied in the rest of the chapter for different types of smart appliances devices. Section 5.3 focusses on smart televisions (TVs) and is divided in sections for data collection, presentation coding, and findings as discussed in Section 5.2. Smart TVs are part of the investigation since it is the most used smart device in a modern home (Kats, 2018). Section 5.3 concludes with a list of security concerns for smart TVs.

The second category of appliances investigated in the study is smart speakers reported in Section 5.4. Smart speakers pose specific risks as its operation depends on the use of the built in microphone and internet connectivity (Securityaffairs.co, 2019). The data collection, presentation and analysis process is again done according to the process discussed in Section 5.2. Section 5.4 concludes with a list of security concerns for smart speakers.

The third category of appliances investigated in this study is smart locks reported in Section 5.5. Locks are used to keep belongings safe and users rely on locks for just this purpose. But network risk factors discussed in Chapter 3 along with security threats and vulnerabilities discussed in Chapter 4 show that smart locks may indeed not be as safe as considered by the unsuspecting homeowner. Once again, the data are collected, presented and analysed as discussed in Section 5.2. Section 5.5 concludes with a list of security concerns for smart locks.

The final appliance category discussed is smart fridges. They have similar characteristics to many other smart appliances such as washing machines, coffee makers, toasters, microwave ovens and other smaller appliances. By investigating the security matters of smart fridges,

guidelines can be compiled for a larger group of appliances. The process outlined in Section 5.2 is presented in Section 5.6 for fridges. Section 5.6 concludes a list of security concerns for smart fridges.

After the discussion of the appliances, gateways are investigated in order to understand the IoT network in a smart from a holistic perspective. Gateways, often referred to as hubs, are the main control centres in homes and may jeopardise the entire home's security, as investigated in Section 5.7.

For each group of the device, a list of security concerns is compiled which is used in the next chapter to create guidelines representative of both the theoretical and empirical investigations of the study. This chapter begins with a discussion of the research strategy which is repeatedly implemented for all the different devices.

5.2 DATA COLLECTION AND ANALYSIS STRATEGY

In this section, the data collection and analysis strategy are discussed to provide a roadmap for the rest of the chapter. The section aims to provide means for an audit trail from data collection to findings. The section starts with a description of data collection, followed by data analysis and coding. The section concludes with a description of the process to develop findings grounded in the data.

5.2.1 Data collection strategy

There are five categories of smart items for which data are collected namely smart TVs, smart speakers, smart door locks, smart fridges, and gateways. In each of the categories, the selection of specific products is based on the biggest brand according to market share. For instance, when it comes to smart TVs, Samsung has a bigger share globally (Reuters, 2018). The likelihood of finding a Samsung smart TVs in people's home today are very high.

Data used in this dissertation come from two sources both of which are in the form of documents, as discussed in Chapter 2, namely data from manufacturers' technical manuals and data from online reviews. Data from manufacturers are viewed as data coming from official documents, and data from reviewers are subjective viewpoints which can be seen as

open-ended interviews without any detail interview questions. The two sources provide two main viewpoints on the data: firstly, the official view of the manufacturer, and secondly, the subjective view of various reviewers.

The reporting process for each category of the device starts with a table that provides background on the type of device, the model, and the manufacturer as indicated by the example Table 5-1. A motivation is provided for the selection of specific the model. Where possible, reviews were linked to specific models within the manufacturer’s range.

Specific references are provided towards to the official documentation of the device provided by the manufacturer. For each device type, only three manufacturers were selected.

Table 5-1 Example of manufacturer data source

Manufacturer	Model	Motivation for selection	Manufacturer documents
S A M S U N G	UN65NU800DEXZA	Samsung is the top global manufacturer of smart TVs with a market share of around 19% (LG, 2012; businessKorea, 2019).	Samsung (2018) Samsung (2019b)

For each chosen device, data are presented in terms of both sources, namely the manufacturer’s documents and reviewer information. Reviewer documentations were collected by following the following process:

- For each device a model was selected to gather reviews for. In many cases, slightly older models of devices were selected to ensure that enough reviews are available to collect valuable data.
- The process starts by searching for a particular term or statement, such as “Sony smart TVs data privacy”;
- From the millions of results from the search, reviews are carefully read to see if they cover the main point required. This is done for a number of reviews until a satisfactory one is found;

- Once the review is selected, it is included in the reviewers' table (discussed below);
- Then a code is created in the first column and a footnote is generated for extra information.

5.2.2 Data presentation and coding strategy

Before the data presentation strategy is discussed for the two types of data, the section provides a summary of the content analysis process followed.

5.2.2.1 Coding strategy using content analysis

Content analysis (as discussed in Chapter 2) is selected as the preferred method for analysing this data. Content analysis involves systematic coding and categorising of large amount of textual information in order to determine trends and patterns. In this dissertation, it is used to code the documents used as data. By using content analysis to analyse the collected data, the data should be able to give a trend or pattern in relation to data security and privacy. According to Stemler (2001:1), any researcher embarking on using content analysing should be able to answer the following six questions:

Q1. Which data are analysed?

A1: *The data analysed is about the security aspects of smart objects used in smart homes.*

Q2. How is the data defined?

A2: *The data are defined based on what each manufacturer says about their smart device/appliances and what reviewers say about the same devices/appliances.*

Q3. What is the population from which the data is drawn?

A3: *The data to be analysed come from electronic documents, which include manufacturers' manuals and online reviews.*

Q4. What is the context relative to which data are analysed?

A4: *Data are analysed in the context of privacy of the people using these smart objects.*

Q5. What are the boundaries of the analysis?

A5: *The analysis is limited to only four different types, smart TVs, smart speakers, smart locks and, smart fridges.*

Q6. What is the target of interest?

A6: *The target of interest are security vulnerabilities and threats posed by smart appliances and devices in a HAN.*

Content analysis goes through three main stages as discussed in Chapter 2, namely preparation, organisation phase, and reporting phases. In the preparation phase the researcher needs to decide on what they want to analyse before selecting a unit of analysis.

In this dissertation, manuals from manufacturers on the items that were to be analysed were studied. For instance, just for one category, smart fridges, manuals from Samsung, LG, and GE were consulted to first understand their contents.

In the next step, which is the organisation phase, the researcher needs to use a qualitative inductive content analysis approach to organise the data, this process allows the researcher to derive variables from such data. This process is known as coding and is demonstrated in the next section and illustrated in Table 5-2 and Table 5-3, where the first column of each table contains codes. By selecting certain units of data, such as sentences or paragraphs, codes were created to summarise statements or paragraphs. This process helps to create links between the research objective and the summary from the raw data. The last step of content analysis is the reporting phase. In this stage, the researcher needs to present his findings. Detail of the strategy for reporting is provided in Section 5.2.3.

5.2.2.2 *Presentation of the manufacturer's documents*

The first source of data namely manufacturer's documents includes technical manuals, user manuals, and privacy policy document on the device. Data for each category of device is presented and analysed in a table, similar to Table 5-2. The table has four columns, the first represents codes developed from the content analysis method chosen for this study, and the other three represent each manufacturer; under each manufacturer, there are three columns with the headings of "Yes, No, and No Comment (NC)". NC represents a situation where the aspect is neither confirmed nor denied in the data.

Table 5-2 Example of coding of manufacturers' documents

Manufacturers	SAMSUNG			LG			SONY		
CODES	YES	NO	NC	YES	NO	NC	YES	NO	NC
VULNERABILITY									
Acknowledges a range of TV sets having a microphone	X				X		X		
THREAT									
Acknowledges sharing of collected data	X			X			X		

For instance, for smart TVs, the code might be “*Acknowledges sharing of collected data*” is classified as a threat. Under the “Yes” headings, the X represents that Samsung, LG, and Sony all agrees to collecting user data via their TV sets.

In order to link the data with theoretical concepts, two categories namely vulnerabilities and threats were identified. These categories align themselves with security issues discussed in Chapter 4, Section 4.5 where security vulnerabilities, threats and attacks are discussed. The codes are grouped according to these categories. It should be noted that a specific code may occur in both categories, as it might be considered both a vulnerability and a threat. The table is followed by a discussion of the data in order to identify vulnerabilities and threats.

The final data representation table for each device presents the coding of the reviewer documents as depicted in Table 5-3 on the next page. The reviewers' table also consists of four major columns, the first column representing the codes, the next three columns represent manufacturers. Under each manufacturer's column, there are sub-columns for reviewers. There are between four to five reviewers per item; this done so that saturation can be achieved by collecting data about the same topic from different viewpoints. In this table, a code coming from a reviewer is represented with a Y[#], where the Y represents the reviewer agreeing to what the code says, then # represents the footnote. Because codes should be short, footnotes

are provided where more detail of what the reviewer said is given. For instance, the code “*Claims that speakers can be hacked to access locally stored data*” that appears under the vulnerability row in Table 5-3 represents statement made by reviewer R1 about Amazon Echo dot, denoted by Y⁴. Reviewer R2 concurs with the views of reviewer R1 hence the notation Y⁵ appearing under the same row. By referring to the relevant footnote, more info is given about reviewer’s statements. Once again, the table is followed by a discussion of the data in order to identify vulnerabilities and threats.

Table 5-3 Coding example of online reviews

Code	Amazon Echo Dot			Google Home		
Reviewer references	R1 (Panda, 2018)	R2 (Symantec, 2019)	R3 (Koch, 2019)	R1 (Panda, 2018)	R2 (Symantec, 2019)	R3 (Koch, 2019)
THREAT						
Claims smart speakers always listening.	Y ¹	Y ²	Y ³	Y ¹	Y ²	Y ³
VULNERABILITY						
Claims that speakers can be hacked to access locally stored data.	Y ⁴	Y ⁵		Y ⁴	Y ⁵	

¹ The reviewer claims that apple, google, and Amazon admit that their smart speakers are always listening to the conversation where they are unless you switch off that function.

² The reviewer claims that the always-listening function of smart speakers scares most people.

³ The reviewer argues that smart speakers represent a new frontier of corporate espionage due to their ability to always listening.

⁴ The reviewer argues that, although the locally stored data is deleted once the speaker realises that you have stopped talking, it takes only a few minutes for a hacker to break into the speaker and steal local data.

⁵ The reviewer confirms that smart speakers can be hacked.

5.2.3 Strategy for the formulation of findings

The findings from the data analysis process assist in understanding the security risks smart appliances may have on data privacy of users. In this section, the aim is to identify security concerns for each category of device. The data from the manufacturer's documents are first summarised as a set of security concerns. The term security "concern" represents both vulnerabilities and threats and possible attacks as this distinction is dependent on context which is sufficiently described in the documents under investigation.

The data analysis from the reviewers' documents are then also summarised as a list of security concerns. These two lists (from manufacturer's and reviewers' documents) are then consolidated and sorted according to the layers architecture model presented in Chapter 3, Section 3.8. The layers are (1) perception or data gathering by means of sensors; (2) network connections, including different protocols; (3) Supplier of cloud and other storage services; and (4) application layer representative of user interfaces. The final summary list is used in Chapter 6 to develop device specific guidelines.

5.3 SMART TELEVISIONS

Samsung (2019g) describe a smart television (TV) as a TV with internet connection and ability to install applications. This short description gives a picture of what a smart TV is, but behind all this, any smart TV comes with an embedded operating system, as discuss in Chapter 3.

5.3.1 Data collection for smart TVs

The selection process of devices to include in this study is provided in Table 5-4 comes from three TV manufacturers, Samsung, LG, and Sony. These three manufacturers in no way represent the whole smart TV market, since year after year the market is changing; but by analysing data from smart TVs coming from these three brands, we are able to form an understanding of security issues affecting smart TVs. The three brands were selected based on their market share, showing that more of their smart TVs are already in people's homes

as compared to another brand (Reuters, 2018). Among each manufacturer, the size of 55 of 75 inches seem to be range which users buy the most (SamsungNews, 2017).

Table 5-4 Smart TVs data source

Manufacturer	Model	Motivation for selection	Manufacturer documents
S A M S U N G	UN65NU8000DFXZA	Samsung is the top global manufacturer of smart TVs with a market share of around 19% (LG, 2012; businessKorea, 2019). This model is a 4K TV with features that are relevant to this study, such as internet connectivity and voice control. The other factor for selection, as compared to other models such as the UN55NU8000FXZA, is the screen size. According to Samsung, smart TVs with screens bigger than 55 inches are popular than smaller screens. 4K TVs, as well, have seen an increase in demand, contributing to almost 50% of all smart TVs sold in 2017 (SamsungNews, 2017). According to (BusinessWire, 2018), by 2023 there will be more than 600 million 4K TVs sold worldwide. This model was released in 2018. An older model is selected to ensure that enough reviews are available to collect valuable data.	Samsung (2018); Samsung (2019f) Samsung (2019b)
L G	65SM8600PUA	LG is second behind Samsung, with a global smart TV market share of around 12% (Technavio, 2018). The TV model is selected based on similar reasons to Samsung, such as the size and the 4K technology, which seems to be the current trend for many consumers. This model also has many features relevant to the study.	LG (2019a) LG (2019b)
S O N Y	XF75	Sony has the 3rd global market share of smart TVs (Reuters, 2018). The model selected is a 4k UHD, is similar to those selected from Samsung and LG. However, a 75-inch version was selected because it adheres to the criteria being used. There are no smaller versions with voice command functionality. Sony has adopted android TV as its primary engine; thus, it relies on google assistant for voice functionalities.	Sony (2019)

5.3.2 Data presentation and coding

As discussed in Section 5.2 data are presented according to the two sources (manufacturer's documents reviewer documents) in this section. Content analysis is used as discussed in Section 5.2.

5.3.2.1 *Manufacturer's documentations*

The data used in Table 5-5 come from TVs manuals, technical documents, privacy policy documents, and manufacturers' websites. The motivation for the inclusion of different documents is to have comprehensive information about the smart TV, its features, the kind of data it collects, and how this data is protected from intruders. The representation of the data in Table 5-5 is documented in Section 5.2.

Table 5-5 Representation of manufacturer's documentations

Manufacturers	SAMSUNG			LG			SONY		
CODES	YES	NO	NC	YES	NO	NC	YES	NO	NC
VULNERABILITY									
Acknowledges a range of TV sets having a microphone.	X				X		X		
Acknowledges a range of TV sets having a camera.	X				X				X
Acknowledges storing collected data on the TV set or in the cloud.	X			X					X
Acknowledges that not agreeing to the privacy policy document can limit the functionalities of the smart TV.	X			X				X	
Specifies that disabling of personalized recommendations does not stop collection of data on the smart TV's usage.	X				X			X	
Acknowledges giving collected data to third party companies for further processing.			X			X	X		
Acknowledges not collecting and storing data on minors.	X			X			X		
Specifies for how long they store the collected data.		X			X			X	
Acknowledges collecting sensitive information from users.	X					X	X		
Acknowledges collection of video footage via the camera on the TV.	X				X				X

Manufacturers	SAMSUNG			LG			SONY		
CODES	YES	NO	NC	YES	NO	NC	YES	NO	NC
Acknowledges collection of TV IP address and device ID by third party companies.	X				X				X
Manufacturer specifies using encryption.	X ⁶				X ⁷				
Manufacturer acknowledges presence of a LAN or Wi-Fi network card.	X			X			X		
Acknowledges TV users can install apps from third party.	X					X			X
Manufacturer specifies using a CPU in the set.	X ⁸					X			X
Manufacturer specifies what OS the TV is using.	X ⁹			X ¹⁰			X ¹¹		
Manufacturer specifies how much RAM the TV set has.	X ¹²				X			X	
THREAT									
Acknowledges that unauthorized access can happen between the communication of the smart TV and company servers.			X	X					X
Acknowledges sharing of collected data.	X			X			X		
Acknowledges using users' collected data.	X			X			X		
Acknowledges collection of data via the set.	X			X			X		

⁶ The TV set support WEP, WPAPSK, WPA2PSK authentication methods, and WEP, TKIP, AES encryption. Samsung advises users to connect their TV set to the wireless HAN using one of the encryptions methods.

⁷ Although LG does not specify what encryption the TV supports, but they leave the decision to connect to a wireless network on the user. They suggest that if the access point uses any kind of security then the user should enter this on the TV.

⁸ Samsung only gives mention of the fact that the set uses a quadcore CPU nothing more on the specifics.

⁹ Although Samsung does not specify it in the TV manual, but they specify on their developer website (Samsung, 2019d) that smart TVs are using Tizen OS.

¹⁰ LG acknowledge that their smart TVs are using WebOS.

¹¹ Sony acknowledges that the TV set is using Android TV OS.

¹² Samsung argues that every TV set may have a different amount of RAM, but in their help documentation they specify the steps a user can take to view the amount of RAM.

Manufacturers	SAMSUNG			LG			SONY		
CODES	YES	NO	NC	YES	NO	NC	YES	NO	NC
Admits collecting basic information, such as channels viewed, menu clicked, and apps accessed.	X			X			X		
Admits collecting voice information via the TV set.	X			X					X
Specifies that marketing companies have abilities to connect to your TV set.	X				X				X
Acknowledges the sale of user data to third parties.			X			X		X	
Acknowledges sharing collected users' information with the authorities, such as the police, when required.			X			X	X		
Acknowledges collecting sensitive information from users.	X					X	X		

1.1.1.1.1 *Discussion of Vulnerabilities*

From the coding data in Table 5-5 we have an insight into the vulnerabilities that smart TVs from these three manufacturers pose.

For instance, with Samsung, the company has acknowledged that this model of smart TV under review is equipped with a microphone allowing users to control the set via voice commands, other models even come with a video camera. The TV set can collect viewers' usage data, device information, such as IP address, audio and video data (only for sets equipped with a camera). Data on minors though is not collected. Samsung has given users the ability to turn off certain data collection features on their TV sets, but they warn them about limiting smart capabilities of the set in the process. The TV has Wi-Fi support allowing it to connect to the internet, which such a feature, the TV transmitted all collected data to the cloud where it is saved on servers. Some of this data can be shared with other companies for other purposes. The duration of the data storage is not mentioned, neither is the security used to transmit and store this data.

The next smart TV reviewed is from LG, although it differs in features compared to Samsung, such as lack of a microphone, they both possess some similarities. For instance, LG acknowledges collecting data via the TV set, this data may include device information and users viewing data. Since the set might not have a microphone, there is no mention of voice data being collected. As with Samsung, LG claims not to collect data on minors. With internet capability of the smart TV, all the data collected is saved on LG's servers in the cloud. There is no mention by LG as to how long such data is stored and if LG shares such data with other companies.

The third smart TV model is from Sony, it has a lot of similarities when compared to Samsung's smart TV in term of features, such as microphone and Wi-Fi support. Sony acknowledges collecting data on viewing behaviours, some of this data may end up being shared with third-party companies for further processing. The company also acknowledges that collected data may be used for tailoring users' adverts. As in the case of other smart TV manufacturers, the features contained in these TV sets are exploitable, and when these vulnerabilities are exploited by attackers, then lead to security threats.

1.1.1.1.2 ***Discussion of Threats***

Samsung acknowledges the collection of user data. These include data about viewing behaviours of users to voice data. The TV set not only allows Samsung to collect data, but they also allow marketing companies to be able to collect data as well. This is a real threat to user's privacy since these other companies might not have the same level of security that Samsung is able to provide to its users. Although Samsung does not say whether this collected data is sold to third party companies, it does acknowledge sharing data sometimes. On the previous privacy policy, Samsung did acknowledge that smart TVs equipped with microphones can also be used to collect sensitive information. Samsung was quick to modify its policy to remove this quote. This raised a lot of questions as to what "collecting sensitive data" meant. The privacy policy might have been altered, but the threat being posed smart TVs to users' information privacy remains a real threat. Samsung is very much aware of the fact that unauthorised access to these TVs is very possible.

LG did not provide enough information as to how data is protected once it leaves the smart TV. One aspect they do acknowledge, is that unauthorised users can intercept the communication between the smart TV and the company servers. LG also accepts that they share some of the collected information with other companies, such as advertisers. The threat users are facing are twofold. First of all, even if data is collected with users' consent, it is still at risk of being compromised if LG does not implement proper security measures. Secondly, an attacker can still exploit any vulnerabilities that may exist from poor network security or host-based security.

Sony acknowledges collecting user data via the TV set, which they can share with third-party companies for advertising purposes. The company documents only specify that basic information is collected, such as viewing information, application access and TV settings. Although the smart TV has a microphone, Sony does not mention anything about collection of voice data via the TV set. The company recognises though that they may collect sensitive data but does not specify what that data includes. Any type of data either audio or another format that is collected from users and classified as sensitive is a serious security risk to the privacy of the users. What is more dangerous is the fact that Sony can share the data they collect with authorities should a subpoena be obtained. Reviewer's documents are presented in coded in next subsection.

5.3.2.2 *Reviewers' documentations*

Table 5-6 represents data from online reviews. Section 5.2 provides a detail explanation as to how the table is compiled and what each entry represents. Of the thousands of reviews found online, these selected reviews cannot represent the views of everyone, but the data collected from these reviewers has helped to have an understanding of the security issues facing smart televisions today.

Table 5-6 Data from Reviewers on smart TVs

Manufacturer	SAMSUNG					LG					SONY				
Reviewer reference	R1 (Matyszczyk, 2015)	R2 (Tsukayama, 2017)	R3 (Raphael, 2015)	R4 (Willcox, 2018)	R5 (Brandom, 2017)	R1 (Matyszczyk, 2015)	R2 (Tsukayama, 2017)	R3 (Raphael, 2015)	R4 (Willcox, 2018)	R5 (Brandom, 2017)	R1 (Cyware.com, 2019)	R2 (Tsukayama, 2017)	R3 (Raphael, 2015)	R4 (Willcox, 2018)	R5 (Tung, 2018)
VULNERABILITY															
Potential of TV set being remotely controlled.											Y ¹⁴				Y ¹³
Possibility of sensitive information being stolen from the TV.											Y ¹⁴				Y ¹³
No specification of how long data is stored.		Y ¹⁵					Y ¹⁵								
Potential of remote controls being used as listening device.	Y ¹⁶	Y ¹⁷					Y ¹⁷								

¹³ Vulnerability discovered in Bravia range of TVs and other Sony smart TVs revealed a command injection flow that could allow someone to run a command remotely with administrative privileges and with no authentication required once connected to the local network.

¹⁴ A vulnerability discovered in Bravia smart TVs range could allow an attacker to retrieve photos and Wi-Fi password stored on the TV.

¹⁵ Stipulates that Samsung and other smart TV manufacturers don't say for how long they keep collected data on their servers.

¹⁶ Acknowledges that remote controls do have a microphone as well with voice recognition capabilities like any smart device.

¹⁷ Acknowledges the potential of the microphone on the remote being used as a potential listening device.

Manufacturer	SAMSUNG					LG					SONY				
Buyers less informed on data privacy.			Y ₁₈					Y ₁₈					Y ₁₈		
Inclusion of privacy document with TV set gives the manufacturer the right to collect data.			Y ₁₉					Y ₂₀					Y ₂₀		
THREAT															
Users put at risk from collected data.	Y ₂₁		Y ₂₁	N ₂₂					N ₂₂					N ₂₂	
Possibility of collected data being used by unknown entities.		Y ₂₃	N ₂₄				Y ₂₃	N ₂₄							
Possibility of collected data being used against the user.		Y ₂₅					Y ₂₅								

¹⁸ Argues that although users have knowledge of the presence of a microphone or camera on the TV set, they don't fully understand what they have agreed to share with the company.

¹⁹ Argues that the inclusion of a privacy document with a smart TV, means you have given the right or consent to the Samsung or any smart TV manufacturer to your private data.

²⁰ Argues that although users have knowledge of the presence of a microphone or camera on the TV set, they don't fully understand what they have agreed to share with the company.

²¹ Argues that every time we commit data to any kind of technology, such a smart TV, there is a possibility of it being stored, and there is an increased potential for errors and carelessness in handling this data, which in turn put users at risk.

²² The reviewer argues that these features can be disabled by providing steps on how data collection can be turned off on many latest smart TVs from popular manufacturers.

²³ Argues that although manufacturers may give options to disable some of the data collections features, taking this route that limit certain smart functionalities on the TV set, or even prevent a setup from completing.

²⁴ The reviewer argues that these features can be disabled by providing steps on how data collection can be turned off on many latest smart TVs from popular manufacturers.

²⁵ Stipulate that data from voice can be taken out of context and used against the user.

Manufacturer	SAMSUNG					LG					SONY				
Samsung agreed to collecting sensitive information via TV sets.	Y ²⁶		Y ²⁷												
Potential of TV set being remotely controlled.											Y ²⁸				Y ²⁸
Possibility of sensitive information being stolen from the TV.											Y ²⁹				Y ²⁹
Potential of collected data being shared with authorities.			Y ³⁰					Y ³⁰					Y ³⁰		

1.1.1.1.3 Discussion of Vulnerabilities

Reviewers acknowledge that Samsung smart TVs come with microphones both in the TV set and the remote control. They argue that the presence of these microphones is a vulnerability since they can be used as listening devices. The remote is able to process voice commands like any other smart devices. The voice recordings from both the remote and the TV are also saved on Samsung servers in the cloud. Reviewers argue that most users are aware of the presence of these microphones and what their purposes are, but the majority don't understand what they have agreed to share with Samsung. They argue that as long as a privacy policy

²⁶ The original privacy policy on smart TVs from Samsung, had a section where they acknowledged that the smart TV may collect sensitive information.

²⁷ As long as the TV can collect voice data, it is difficult to know what type of data it is collecting, thus some personal or sensitive data may be collected in the process.

²⁸ Vulnerability discovered in Bravia range of TVs and other Sony smart TVs revealed a command injection flow that could allow someone to run a command remotely with administrative privileges and with no authentication required once connected to the local network.

²⁹ A vulnerability discovered in Bravia smart TVs range could allow an attacker to retrieve photos and Wi-Fi password stored on the TV.

³⁰ Stipulate that the information collected via smart TVs, not only is it shared with third party companies for advertising purposes, but it can also be handed over to the authorities if the government has a subpoena.

document is included with a TV set, the user has already given Samsung the right or consent to their private data, whether the user read the document or not.

With regard to LG smart TV, as long as the set can connect to the internet and data is collected via it and stored online, it already put the user of the TV at risk of the set being compromised and used for other malicious purposes. Viewing data can reveal a lot about the behaviour of users in the house, as to when they are home or away. The challenge of most smart TV manufacturers, including LG, is that they don't inform users enough on data privacy. Users need to be given a chance to make an informed decision without being coerced to give up their information in exchange for the features offered by the TV.

Every device that uses an operating system and is able to connect remotely to the internet, is at risk of being attacked. There is a need for manufacturers to ensure that security is part of the fabric of the smart TV. This sometimes becomes a challenge especially when the operating system being used comes from google. If there is any vulnerability in the operating system that is exploited, then the blame can't rest only on Sony. When it comes to data collection, some reviewers argue that users should be able to disable data collection options, but as was discussed before, by disabling certain features on the TV does limit the smart capabilities of the TV. For instance, the data collected is used to improve the services being provided, and for many manufacturers the more data they collect from users the better the services the TV can provide. It becomes almost impossible for TV manufacturers, such as Sony, not to collect data from users. This data can be used to improve the type of contents they offer, it can also give them good feedback from users. The most important part of data collection is to let users know what is being collected and for what purpose it will be used for. As one reviewer mentioned, users need to be well informed about the privacy policies of the TV set they purchase.

1.1.1.1.4 ***Discussion of Threats***

Any type of data collection put people privacy at risk if the data is not protected. Smart TVs are able to collect data in abundance and the majority of which is stored online. For these devices to come equipped with powerful microphones, sometimes even cameras raise the risk even higher for the type of data they collect. There is always a possibility of this data

ending up in the wrong hands no matter how good the company may claim to protect it. It is true that other devices such as cell phones and tablets already generate a lot of data which at times is given willingly. The hardware advancement on these devices has made sure that they can be able to provide better data protection via encryption and use of antiviruses to scan for malicious software. This though becomes a challenge for devices with limited hardware. Samsung once claimed to collect sensitive information via the TV set. For the fact that smart TVs have means of recording audio and even video, would sensitive information include private conversations taking place in someone's sitting room? Of course, the TV can be switched off if you don't want it to record sensitive information, but as shown by the weeping angel exploit, it is very possible to still record audio with a TV that is pretending to be off. Although this exploit was tested on a different model of Samsung TV, it still raises a lot of questions to the kind of threat these TV sets pose for an ordinary home user. There is a high possibility that a TV set could be used to collect information on people, and this information can be shared with the authorities when needed.

Security of smart TVs can be provided both in the software, e.g. operating system and in the TV hardware. LG smart TVs use their own operating system which provides features comparable to any operating system found on mobile devices. The ability to connect to the internet and collect users' data means better security needs to be provided. Their smart TV range also is not any better than what the competitors provide. They are all susceptible to being compromised by unauthorised individuals. The threat still rests on the amount of data they collect and how this is protected. Not everyone that will be using the TV is knowledgeable about the security danger such a device can pose to the confidentiality and privacy of one's home. Hence it is important to be aware of the type of data collected and of the possibility of such data ending up in the wrong hands.

Sony smart TVs, especially the Bravia range, make use of Android TV software. Android as an operating system has its shares of security flaws that are discovered from time to time. These televisions come with preinstalled applications which may also introduce another layer of security flaw in addition to the OS. In 2018 a number of Sony Bravia TV models were discovered to have a vulnerability that could allow an attacker to remotely run a command

with administrative privileges without the need of authentication. Another vulnerability allowed an attacker to copy photos stored on the TV as well as Wi-Fi password keys. T. Bugs in the software are one of the many issues that compromise the security of such devices. Sony made sure a patch was released to fix these loopholes. The potential for such vulnerabilities to be exploited into an attack before they are discovered is very much possible. This highlights the importance of TV manufacturers to ensure the software they release are thoroughly analysed for such vulnerabilities. Sometimes software may come from other developers with less stringent security checks. The report also mentions that these attacks are only possible if the attacker could be on the same network as the TV. This shows that the security of the network where the smart TV is deployed is vital to the overall security of the TV, and in extension to the integrity and privacy of users. These flaws are proof that any other type data may be stolen from these TV sets. It is worse when the set are equipped with microphones and they are able to record also audio and store them on the TV.

5.3.3 Smart TVs findings

In this section the security concerns discussed in terms of vulnerabilities and threats identified in the data are summarised and combined from the two data sources. The aim is to identify specific concerns that needs to be taken into account in the development of guidelines for home owners regarding security concerns in smart homes, developed in Chapter 6.

The following concerns were identified from manufacturer's documents as discussed in the previous section:

- Collection of data on users' viewing habits;
- Collection of sensitive data;
- Presence of microphone;
- Possibility of data transmission being intercepted;
- Storage of users' data on server in the cloud;
- Sharing of data with third parties.

The following threats were identified from reviewers' documents as discussed in the previous section:

- Sharing of data with third-parties;
- Possibility of the data falling into wrong hands;
- Lack of security knowledge by device users;
- Lack of knowledge of privacy policy of users;
- Different manufacturers have different OS with different features
- Operating systems used prone to attacks;
- Presence of security loopholes in software;
- Lack of stringent quality control of third-party software by manufacturers.

These lists may be combined into a single list of security concerns of smart TVs from the empirical investigation:

- Collection of sensitive data;
- Presence of microphone;
- Possibility of data transmission being intercepted;
- Storage of users' data on server in the cloud;
- Sharing of data with third parties;
- Possibility of the data falling into wrong hands;
- Possibility of data transmission being intercepted;
- Operating systems used prone to attacks;
- Presence of security loopholes in software;
- Lack of security knowledge by device users;
- Lack of stringent quality control of third-party software by manufacturers;

These security concerns are compared with generic concerns in Chapter 6, and where appropriate, device specific guidelines are formulated for smart TVs.

5.4 SMART SPEAKERS

Smart speakers are wireless voice-controlled speakers, with the ability to understand voice commands and able to execute certain functionalities, as discussed in Chapter 3. Speakers are equipped with speakers and microphones and some models have built-in cameras. Speakers are sometimes used as user interface devices for gateways.

5.4.1 Data collection for smart speakers

Data sources for smart speakers come from three of the largest manufacturers of smart speakers globally according to market share as shown in Table 5-7. These speakers in no way represent the whole spectrum of smart speakers out there, but the data obtained is enough for us to have an understanding on the security issues smart speakers are facing.

It should be noted that smart speakers are still a new technology, some manufacturers only have one version of the device, such as in the case of Apple. Hence there is no other model to select from.

5.4.2 Data presentation and coding

Data presented in this section come from two sources as discussed in Section 5.2, manufacturers' documents and reviewers' documents. Content analysis was used as discussed in Section 5.2.

5.4.2.1 *Manufacturers documentations*

The data in Table 5-7 come from documents from manufacturers, these include device manuals, privacy documents of smart speakers, and also manufacturers' websites. The representation of this table is explained in Section 5.2.

Table 5-7 Smart speakers data source

Manufacturer	Model	Motivation for selection[#]	Manufacturer documents
A M A Z O N	Echo	By 2018 the USA alone had almost 118 million smart speakers in users' homes (Sterling, 2019). Amazon alone claims to have sold around 100 million Echo smart speakers worldwide (Leary, 2019). The Echo model seems to be the most popular smart speaker from Amazon. Also Amazon is currently the leader in the number of smart speakers sold to date (Owen, 2019).	Amazon (2019c)
G O O G L E	Home	Google Home is the second most sold smart speaker, according to published reports (Owen, 2019). By the end of 2018, almost 11 million google home smart speakers were sold.	Google (2019a)
A L I B A B A	*Tmall genie	Although Amazon and Google seem to have a big market share in the USA and Europe (Thestaronline.com, 2018), Chinese smart speakers prove popular at home. Alibaba's Tmall genie speakers had almost 41% sales share in Q4 of 2018 in China (Kinsella, 2019). Also, Alibaba is the 3 rd largest supplier of smart speakers globally (Owen, 2019).	Not included [#]
A P P L E	Homepod	Apple Homepod is added to this list because Apple produces premium products. Although it might be 6 th globally, it is 3 rd in the USA, and the brand is well known also globally as compared to Chinese brands which are currently only popular locally.	Apple (2019)
[#] The Tmall genie has more devices in circulation than Apple's Homepod, but it is not included further due to lack of information. No data from the manufacturer or reviews could be easily obtained.			

Table 5-8 Representation of manufacturers' documentations

Manufacturers	AMAZON			GOOGLE			APPLE		
Model	Echo Dot			Home			Homepod		
Codes	YES	NO	NC	YES	NO	NC	YES	NO	NC
VULNERABILITY									
Acknowledges speaker having a microphone.	X			X			X		
Acknowledges the capability of the device to connect to the internet.	X			X			X		
Acknowledges that the smart speaker can be used to control other compatible smart appliances.			X			X	X		
Acknowledges that the speaker is always listening.	X			X			X		
Acknowledges exchanging information with third party services that a user may connect to with permission from a user.			X	X					X
Acknowledges storing collected data from smart speakers on their servers.	X			X					X
Acknowledges the speaker having the function to mute the microphone.	X			X					X
Acknowledges that despite the microphone always being on, the speaker can only start recording after a key phrase has been said.	X			X			X		
Provides the ability to delete what the speaker has learned about the user during usage.			X	X					X
Manufacturer specifies the OS the speaker is running.		X			X				X
Specifies how much RAM the speaker has.		X			X				X
Manufacturer specifies the type of encryption the speakers uses.		X		X					X

Manufacturers	AMAZON			GOOGLE			APPLE		
Model	Echo Dot			Home			Homepod		
Codes	YES	NO	NC	YES	NO	NC	YES	NO	NC
Specifies the CPU being used by the speaker.			X		X		X ³¹		
THREAT									
Acknowledges that the speaker is always listening.	X			X			X		
Acknowledges collecting information on the usability of the service by users.			X	X			X		
Acknowledges storing collected data from smart speakers on their servers.	X			X					X
Acknowledges storing a recording of voice commands to improve the functionality of the service.			X	X					X
Acknowledges that recorded voice commands can be deleted by the user.	X					X			X
Acknowledges the speaker having the function to mute the microphone.	X			X					X
Acknowledges that despite the microphone always being on, the speaker can only start recording after a key phrase has been said.			X	X			X		
Acknowledges collecting of data, such as devices IP addresses, user location.	X			X					X
Provides the ability to delete what the speaker has learned about the user during usage.			X	X					X
Acknowledges encrypting conversations stored locally on the device.			X	X					X

³¹ Apple acknowledges that the smart speaker is using an A8 processor

1.1.1.1.5 ***Discussion of vulnerabilities***

Smart speakers from the three manufacturers have certain features in common. For instance, the most common features of a smart speaker include a powerful microphone, internet connectivity, an operating system, a digital voice assistant, and reliance on server services in the cloud. All the three smart speakers have microphones with the capability of always listening, but the three manufacturers argue that these speakers can only start recording once they hear a key phrase. For instance, the key phrases may be “*Hi Alexa*”, “*Hi Google*”, or “*Hi Siri*” respectively. On all the three speakers, users have the ability to switch off the microphone if they don’t want it to hear the conversation in the room.

When it comes to data collection, all the three manufacturers agree to collecting various type of data via the speakers, this may include commands sent to the speaker, or any kind of voice that the speaker is able to record, and also data about the device itself. Collected data is stored on servers in the cloud. The speakers also have the ability to store data locally. In the case of Amazon, there is not mention if the transmitted or the locally stored data is encrypted or not. Neither Amazon, Google nor Apple mention for how long the data is stored on their servers. Echo and Home speakers both store some local data, but there is no mention on Homepod about locally stored data. Google is the only one that acknowledges that users are able to delete the data that speaker has stored locally; they also claim that this data is encrypted.

1.1.1.1.6 ***Discussion of threats***

The always-listening feature of these speakers can be a threat as much as it can be a vulnerability. Amazon claims to store data on their servers, although not specifying for how long, but according to reviewers this data is kept permanently on these servers. It is true that users may not be aware of just what type of information about them may have been stored on the internet. No matter how good a company claims its server security to be, yet there is always news about servers being broken into and information leaked or stolen. Hence the collection of data via the speaker and storage of it in the cloud poses a threat to the privacy of users themselves.

Google claims to collect data via the speaker, which is then stored in the cloud. Just like Amazon, Google is not specific for how long they keep this data, but some reviewers claim

it is permanently stored. The speaker, with its powerful microphone, does collect mainly voice commands that users pass to it. For the fact that it has a microphone, it can also record other conversations. Apart from voice recorded data, Google also acknowledges collecting data on the usability of the speaker as well as other information. Technically, recorded commands can be replicated by intruders to simulate authentic commands.

Of the three smart speakers, Apple's Homepod seems to be the only one with voice capabilities that are not as advanced as Google and Amazon. Siri, which is the voice assistant used on Homepod, is not as advanced as the other two competitors. Despite these limitations, Apple claims the Homepod to be a very secure smart speaker. The speaker shares similar features with the competitors on how they handle user data as compared to amazon and google. Apple claims to collect user data via the speaker which also include voice commands. The speaker can be used to do online shopping on the internet, thus the type of data collected may also involve very confidential information, such as ID numbers, bank accounts, or credit card number. Apple confirms that encryption is used to make sure transmitted data between the speaker and the servers in the cloud is protected.

5.4.2.2 *Reviewers documentations*

Reviewers' data are represented in Table 5-9, the format of the table and how data is entered is explained in detail in Section 5.2. The reviews in this table in no represent the opinion of every reviewer, but they offer an insight on the security issues facing smart speakers.

Table 5-9 Representation of reviewers' documents

Manufacturer	Amazon Echo Dot			Google Home			Apple Homepod		
Reviewer references	R1(Panda, 2018)	R2 (Symantec, 2019)	R3 (Koch, 2019)	R1 (Panda, 2018)	R2 (Symantec, 2019)	R3 (Koch, 2019)	R1(Panda, 2018)	R2 (Symantec, 2019)	R3 (Koch, 2019)
VULNERABILITY									
Claims risk of a software bug.	Y ³²			Y ³²			Y ³²		
Claims that Homepod can accept “Hi Siri” command from anyone, including strangers.							Y ³³		
Smart speakers can be an entry point for hackers.		Y ³⁴			Y ³⁴			Y ³⁴	
Confirms that speaker store voice recordings permanently.	Y ³⁵	Y ³⁶	Y ³⁷	Y ³⁵	Y ³⁶	Y ³⁷			
THREAT									

³² The reviewer claims that there is always a risk of a bug in the software, but users need to make sure they download updates to patch these vulnerabilities.

³³ The reviewers argue that allowing anyone to use the “Hi Siri” command is a security risk to users' data because it can allow anyone to get access to one's diary, or even make a phone call.

³⁴ The reviewer argues that, because a smart speaker can act as a hub in a smart home, it can become a single point of vulnerability through which an attacker can get access to other devices in the network.

³⁵ The claims that Google and Amazon stores voice recordings from smart speakers permanently, to improve advertising.

³⁶ Claims that you might not know who else has access to the information stored on the servers, and what they can do with it.

³⁷ The reviewer argues that Amazon stores voice recording from their smart speaker on servers forever.

Manufacturer	Amazon Echo Dot			Google Home			Apple Homepod		
Claims that speakers can be hacked to access locally stored data.	Y ³⁸	Y ³⁹		Y ³⁸	Y ³⁹		Y ³⁸	Y ³⁹	
Claims that Homepod can accept “Hi Siri” command from anyone, including strangers.							Y ⁴⁰		
Claims smart speakers always listening.	Y ⁴¹	Y ⁴²	Y ⁴³	Y ⁴¹	Y ⁴²	Y ⁴³	Y ⁴¹	Y ⁴²	Y ⁴³
Claims speakers to be relatively secure.							Y ⁴⁴		
Claims speakers support two-way authentication.							Y ⁴⁵		
Claims most people fear the recording capabilities of smart speakers.	Y ⁴⁶			Y ⁴⁶			Y ⁴⁶		
Argue that Homepod recordings are anonymous.							Y ⁴⁷		Y ⁴⁸

³⁸ The reviewer argues that, although the locally stored data is deleted once the speaker realises that you have stopped talking, it takes only a few minutes for a hacker to break into the speaker and steal local data.

³⁹ The reviewer confirms that smart speakers can be hacked.

⁴⁰ The reviewers argue that allowing anyone to use the “Hi Siri” command is a security risk to users’ data because it can allow anyone to get access to one’s diary, or even make a phone call.

⁴¹ The reviewer claims that Apple, Google, and Amazon admit that their smart speakers are always listening to the conversation where they are unless you switch off that function.

⁴² The reviewer claims that the always-listening function of smart speakers scares most people.

⁴³ The reviewer argues that smart speakers represent a new frontier of corporate espionage due to their ability to always listening.

⁴⁴ The reviewer claims that smart speakers from Amazon, Apple, and Google use WPA2 for encrypting wireless communication preventing hackers from intercepting traffic.

⁴⁵ Two-factor authentication requires that a trusted device, such as a cell phone, can authorise a purchase made via a smart speaker via a code that is sent to it.

⁴⁶ The reviewer claims that most people fear smart speakers because they don’t know what they are recording and where the data is going.

⁴⁷ The reviewer argues that, according to apple, all voice recordings via the speaker are anonymous, meaning you would not tell who made the recording.

⁴⁸ The reviewer claims apple’s Homepod recordings are not linked to the user’s account.

Manufacturer	Amazon Echo Dot			Google Home			Apple Homepod		
Confirms Apple Homepod stores recordings for a short period.							Y ⁴⁹		Y ⁵⁰
Confirms that Google and Amazon store voice recordings permanently.	Y ⁵¹	Y ⁵²		Y ⁵¹	Y ⁵²				
Anything the speaker misunderstands is still recorded and saved on servers.			Y ⁵³			Y ⁵³			Y ⁵³
Voice recordings on Echo Dot and Google's home are linked to the user's account.			Y ⁵⁴			Y ⁵⁴			
Addition of extensions result in more user data to be collected.			Y ⁵⁵			Y ⁵⁵			

1.1.1.1.7 *Discussion of vulnerabilities*

The ability of the speaker to always be in listening mode put the owner at risk if the speaker is accessed by an attacker. The speaker can be used for eavesdropping, or the locally stored voice recordings can be accessed. Although Amazon does not specify for how long they store collected data, reviewers claim that the data is never deleted, and it is stored permanently. This really poses a security risk, the data can be leaked, or the server can be compromised. The operating system or software used in these speakers can always contain security bugs, and when these are exploited, the speaker itself can become an entry point into the network.

⁴⁹ The reviewer argues that voice recordings from the apple's Homepod are only stored for six months.

⁵⁰ The reviewer claims that, of the three smart speakers, only apple's Homepod is the only one that does not keep the recordings permanently.

⁵¹ The reviewer claims that Google and Amazon store voice recordings from smart speakers permanently, to improve advertising.

⁵² Claims that you might not know who else has access to the information stored on the servers, and what they can do with it.

⁵³ The reviewer claims that if a user says something that the speaker misunderstands, that information is still recorded and stored on the servers forever.

⁵⁴ The reviewer claims that both Google Home and Amazon Echo speakers' recordings are linked with user account registered on the device.

⁵⁵ The reviewer claims that Google Home and Amazon's Echo Dot permit third-party extensions that connect the speaker to other applications. These extensions result in more user data being collected by third parties. The only speaker not to allow this is the apple's Homepod, thus it is more private and secure than the other two.

Google Home's ability to always be in listening mode is a vulnerability that can be exploited by hackers. For one, the powerful microphone on the speaker can be turned into an eavesdropping device by a hacker. Reviewers also claim that voice recording from these speakers is kept permanently on the servers. This poses a security risk should hackers get access to these servers. The operating system and software used on these speakers are not error-proof; there is always a possibility of a software bug that can be exploited maliciously by hackers allowing them to access and locally stored data. Google home though has a layer of protection built into the speaker, should it be hacked. That is, the locally stored data is encrypted. If the speaker was placed in an unsecured network, and it happens that someone can hack into the speaker, they will have to find a way of decrypting the data for it to be of any use. For Google and any giant tech company, these speakers are really a perfect data mining tool. Unfortunately, this data can also land in the wrong hand and being misused. Unlike apple that does not link the recording with a user account, thus keeping them untraceable, all voice recording done on a google home speaker is linked to an email account, which makes it easy to trace back to who the owner is.

Reviewers do agree with Apple's statement about the speaker being safe. Although the documentation shows that the speaker is always in listening mode, some reviewers disagree. Homepod uses a single user ID, unlike the other two that use multiple user accounts. One feature that reviewers consider the Homepod to provide better security than its competitors is the fact that recordings are not linked to any user account. Thus, they remain unanimous. Although Apple did mention anything about how long data is stored on their servers, some reviewers claim that the data is kept only six months. Apple, like other big tech companies, focuses on data collection to enhance a lot of their services. The massive amount of data collected stored online poses a security risk to the privacy of many users. Should the data fall in the wrong hands, or even if the company itself decides to exploit this data at the benefit of the user, this can put the privacy of users at risk.

1.1.1.1.8 *Discussion of threats*

Certain implementations and decisions by the manufacturers concerning the smart speaker put users at risk and present a real threat to the security and privacy of users' data. Amazon stores users' data permanently in the cloud. The speaker also stores data locally until the user can delete it. Although the speaker seems to provide some degree of security, reviewers claim that their security can still be compromised may be due to a bug in the software, which may also come from third-party plugins that can be installed. These plugins may even increase the amount of data collected. At times some of the collected data by third parties may not be secured the same way Amazon does it.

For as long as a smart speaker can connect to the internet, it is already at risk of being attacked and compromised. According to reviewers, all smart speakers pose this risk. Google Home speaker collects numerous types of data, which include voice recordings. Some of these recordings are stored locally on the speaker. According to reviewers, this data can be accessed by an intruder, but other reviewers claim that google home encrypts all locally stored data providing confidentiality to the user. Data which is transmitted and stored in the cloud is said to be stored permanently.

Despite the efforts of smart speakers' manufacturers to provide security to home users, they all are vulnerable to security attacks, either via the local network or through a cyber-attack. Reviewers claim that Homepod speakers have one big flaw due to the use of Siri, and that is the speaker can accept the command "hi Siri" from anyone even a stranger. This poses a real threat; this means anyone could access the speaker and its data via voice commands. The good thing about vulnerabilities that pose security threats is that manufacturers can close them through software patches. Although some reviewers claim that the speaker is always listening, Apple does not mention anything concerning this. Although the speaker may only record once the user says the key phrase "hi Siri", the fact that the speaker has a very powerful microphone still poses a real security threat to users. Encryption does indeed provide confidentiality, but some attacks may not necessarily involve stealing the data stored on the speaker. An intruder may at times target the speaker and make use of the powerful microphone for eavesdropping purposes. Smart Speakers Findings

In this section findings for smart speakers are presented according to the strategy presented in Section 5.2.

5.4.3 Smart Speaker findings

In this section the security concerns discussed in terms of vulnerabilities and threats identified in the data are summarised and combined from the two data sources. The aim is to identify specific concerns that needs to be taken into account in the development of guidelines for home owners regarding security concerns in smart homes, developed in Chapter 6.

- Always on speaker recording data;
- Storage of collected data in the cloud;
- Replication of user voice commands.

The following security concerns were identified from reviewers' documents as discussed in the previous section:

- Data stored permanently in cloud for long periods;
- Data is stored on the device itself;
- Built-in security lacking;
- Third party plugin software not under scrutiny of manufacturer;
- Intruders may use device to control gateway;
- Misused of stored information.

These lists may be combined into a single list of threats posed by the use of smart speakers:

- Always on speaker;
- Data is stored on the device itself.
- Data stored in cloud for long periods;
- Built-in security lacking;
- Third party plugin software not under scrutiny of manufacturer;
- Replication of user voice commands;
- Intruders may use device to control gateway.

These security concerns are compared with generic concerns in Chapter 6, and where appropriate, device specific guidelines are formulated for smart speakers.

5.5 SMART LOCKS

A smart lock is a network-enabled lock with the ability to be controlled remotely, allowing homeowners to lock and unlock and monitor their doors anywhere. More details on smart lock is given in Chapter 3.

5.5.1 Data collection for smart locks

Among the many smart locks on the market today, only three could be selected for this study as given in Table 5-10. In no way are these three models better than the other brands, but they have features that will help in understanding or have a good understanding of security issues that may affect all smart locks as a whole.

Table 5-10 Smart locks data source

Manufacturer	Model	Motivation for selection	Manufacturer documents
Y A L E	Assure Lock SL with Zigbee	The smart locks listed in this section are selected from the list of the best ten smart locks for 2019 according to a review done by Delaney (2019). The main selecting factors are the smart features that these locks can offer such as: • the ability to connect to the internet; • the ability to be controlled remotely; • the ability to be controlled using voice activation using smart speakers such as google home or Amazon's Echo dot;	Yale (2019)
A U G U S T	Smart Lock Pro Connect		August (2019b) August (2019a)

S C H L A G E	Sense™ Smart Deadbolt Z-Wave plus	geofencing or location services which allow homeowners to unlock their doors once the lock detects a trusted device (cell phone) nearby. It is to be noted that August was bought by Yale, thus the modules that provide smart features in Yale's smart locks are actually August modules. Having said that, it means the privacy policy that applies to August is the same as the one applying to Yale's smart locks.	Schlage (2019)
--	--------------------------------------	---	----------------

5.5.2 Data representation and coding

In this section, data from manufacturers and from reviewers is coded and presented in table format.

5.5.2.1 *Manufacturer documentations*

The data in Table 5-11 come from documents from manufacturers, these include device manuals, privacy documents of smart speakers, and also manufacturers' websites. The representation of this table is explained in Section 5.2.

Table 5-11 Representation of manufacturer's documentations

Manufacturers	Yale			August			Schlage		
Codes	YES	NO	NC	YES	NO	NC	YES	NO	NC
VULNERABILITY									
Acknowledges that the lock can connect to the internet when a compatible IoT hub is used.	X			X			X		
Acknowledges that users can control the lock from anywhere.	X			X			X		
Ability to grant secure access to guests, family and friends.	X			X			X		
Acknowledges storing personal data on servers.	X			X					X
Acknowledges collecting data about people who lock/unlock the door.			X	X					X

Acknowledges storing personal data on servers.	X			X			X		
Acknowledges collecting data about guests that have been given access to the lock.			X	X					X
Acknowledges collecting data about lock status.	X			X			X		
THREAT									
Acknowledges storing personal data on servers.			X	X					X
Acknowledges collecting data about people who lock/unlock the door.			X	X					X
Acknowledges collecting data about guests that have been given access to the lock.			X	X					X
Acknowledges that the lock app may require access to geolocation information but argues that the data is never saved on the servers but locally.	X			X					X
Acknowledges that collected data may be shared with third-party companies.	X			X					X

1.1.1.1.9 *Discussion of vulnerabilities*

Yale's offering of smart locks come with support for various wireless connectivity, Bluetooth, Z-Wave and ZigBee. These network protocols are supported by a network module that can be installed into the lock. The module allows the lock to connect to the internet also when a compatible hub is used. Internet connection on the lock allows it to be remotely monitored and controlled, this includes the user checking the status of the lock, giving access to friends or guests remotely. It can also allow the manufacturer to have to check the status of the lock. The manufacturer agrees that they do collect data about the device status, data about people who open or close the door. The data collected is stored on servers in the cloud.

August produces one of the best smart locks on the market today. As part of Yale, they also produce the network modules that are found in Yale's smart lock. August locks support several network protocols, among them ZigBee, Z-Wave, Bluetooth and Wi-Fi. With network capabilities, the smart is able to connect to the internet and offer the user all kind of smart features, such as remote lock and unlock the door, automatic unlocking using

geosensing. August admit to collecting various forms of data, from users to the device itself. The data collected may include personal data. All the collected data end up on servers in the cloud where it is stored.

The Schlage Sense is a Bluetooth version which be connected to a Wi-Fi module to add remote functionalities, and the Schlage connect support Z-Wave allowing it to be integrated with other IoT hubs. The Wi-Fi connectivity allows the lock to be controlled using voice command when compatible digital assistants are used, such as Siri, Alexa or Google. Like the competitors, using the mobile app, the owner can grant access to the lock via the use of digital keys, this can allow anyone with the key to enter the house even if the owners are not there. There is no mention from the manufacturer about data collection, they don't admit nor deny if any personal data is collected and stored on servers. The manufacturer though admits to collecting data on the status of the lock.

1.1.1.1.10 ***Discussion of threats***

All the data collected from the lock via the mobile app is stored on servers in the cloud. This data includes information on people who open and close the door, it also includes data about individuals, such as guest that have been given access to open the lock. The data collected include personal information. The manufacturer confirms that the lock can be controlled or monitored remotely. The mobile app for controlling the lock requires access to geolocation data, but they argue that none of that data is stored locally or in the cloud. Geolocation data is used for a feature call geosensing, which allows the lock to automatically open once it senses the phone in the proximity. Data collected through the lock and the mobile application can also be shared with third-party companies.

August admits to collecting the various type of data and storing it on servers in the cloud. Device status data, personal information for guests who are given digital keys to open the door, data on people who enter the house, geolocation data. They also admit that sometimes collected data may be shared with other companies for various reasons.

Schlage, like the other smart lock manufacturers, agrees too to data collection, but little is given as to the type of data they collect and how this data is being used or for how long it is stored.

5.5.2.2 Reviewer's documentation

The data represented in Table 5-12 comes from reviewers' documents. The way the data is represented is explained in detail in Section 5.2.

Table 5-12 Representation of reviewer's documentations

Manufacturer	Yale					August					Schlage			
Reviewer references	R1(Micro, 2014)	R2 (Tomlinson, 2019)	R3 (protectamerica.com, 2018)	R4 (Douglas, 2017)	R5 (Price, 2018)	R1 (Micro, 2014)	R2 (Tomlinson, 2019)	R3 (protectamerica.com, 2018)	R4 (Douglas, 2017)	R5 (Price, 2018)	R1 (Micro, 2014)	R2 (Tomlinson, 2019)	R3 (protectamerica.com, 2018)	R4 (Douglas, 2017)
VULNERABILITY														
An attacker can unlock doors with stolen phone that is connected to the lock.			Y ⁵⁶						Y ⁵⁶					
All smart locks are insecure if users don't know how to use them securely.				Y ⁵⁷	Y ⁵⁸				Y ⁵⁷	Y ⁵⁸				Y ⁵⁷

⁵⁶ The review argues that for locks that support geofencing, where the lock sense an authorized phone and automatically unlocks the door, is a security risk if the phone is stolen. It means an attacker can use the phone to unlock the door.

⁵⁷ The reviewer argues all smart locks are insecure if used in the wrong way, so user education is an important factor.

⁵⁸ According to the reviewer, a vulnerability was found in one of the smart locks that allowed an intruder to use voice command to unlock the door, but this work only if the user did not configure the lock properly. Showing again the need for users to be better trained.

THREAT													
Digital keys stored in the cloud.	Y ⁵⁹					Y ⁵⁹					Y ⁵⁹		
Digital keys may be shared remotely with others.	Y ⁶⁰					Y ⁶⁰					Y ⁶⁰		
Servers in the cloud are prone to cyberattacks.	Y ⁶¹					Y ⁶¹					Y ⁶¹		
Possibilities of attacks on data during transmission.	Y ⁶²	Y ⁶³				Y ⁶²	Y ⁶³				Y ⁶²	Y ⁶³	
Smart locks are prone to cyberattacks.		Y ⁶⁴	Y ⁶⁵	Y ⁶⁶			Y ⁶⁴	Y ⁶⁵	Y ⁶⁶			Y ⁶⁴	Y ⁶⁵
Users need to be made aware of the vulnerabilities of smart lock.		Y ⁶⁷		Y ⁶⁸			Y ⁶⁷		Y ⁶⁸			Y ⁶⁷	Y ⁶⁸
Need for manufacturers to release patches regularly.		Y ⁶⁹					Y ⁶⁹					Y ⁶⁹	

⁵⁹ The reviewer argues that all smart locks vendors store digital keys and other properties of smart locks on servers in the cloud.

⁶⁰ The ability to store keys in the cloud makes it easier for home owners to send these keys remotely to friends or families that may require temporary access.

⁶¹ Since information about smart locks are stored on servers on the internet, attackers can target these servers from any location.

⁶² Network attacks can be used as the smart lock communicate with the server or with the app remotely.

⁶³ Data transmission between smart lock and servers in the cloud, or between smart phone and the lock need to be encrypted to prevent attacks

⁶⁴ Just like any other IoT device, smart locks can be compromised by an attacker

⁶⁵ The review argues that smart locks bring useful convenience to users, but manufacturers need to make sure they release security patches regularly when vulnerabilities are discovered.

⁶⁶ The reviewer argues that all types of smart lock are prone to cyberattacks as long they can connect to a network, and the blame is put mostly on the carelessness of the user.

⁶⁷ Users need to be made aware that their smart lock may be attacked, and they have to be prepared when that happens

⁶⁸ The reviewer argues all smart locks are insecure if used in the wrong way, so user education is an important factor.

⁶⁹ The review argues that smart locks bring useful convenience to users, but manufacturers need to make sure they release security patches regularly when vulnerabilities are discovered.

1.1.1.1.11 ***Discussion of vulnerabilities***

The reviewers argue that a smart lock has the same security issues as any other IoT device found in smart homes today. The vulnerabilities these locks suffer from, come from the many aspects of IoT, such as poor design. IoT devices do generate a lot of data. In the case of smart locks, data on the status of the lock, geosensing data, information on users operating the lock, even digital keys that are remotely shared. All this data ends up being stored in the cloud. According to reviewers, the data is exposed to cyberattacks.

Although data may not be attacked on the servers themselves, while it is being transmitted, there is a high chance of it being compromised, especially if not encrypted. In some part of the world, such as in Europe, users can request that their data be erased from the servers.

August smart locks face the same kind of vulnerabilities that other locks face. For instance, users are unaware of what type of data and how much data is collected from them. The storage of data online put user's information at risk since all servers are prone to cyberattacks. Data can also be compromised if a phone that is allowed to open doors get stolen, the reviewer argues that this will allow an intruder to easily open the door. Another reviewer argues that at times smart locks are vulnerable because homeowners don't know how to use the device, poor configurations may lead to the device is prone to attacks.

Although there is little information on how Schlage collect their data, reviewers argue that all smart locks do collect data in one form or another, and this data ends up in the cloud. The Schlage Sense uses Bluetooth to communicate with the cell phone, but a user might add a Wi-Fi module, as an extra, to allow the lock to be controlled remotely just like the other smart locks on the market. The Schlage Connect is the Z-Wave version of the lock which can connect with other IoT devices via a compatible IoT hub, such as Samsung SmartThings. This integration allows the lock to be controlled via using Alexa or Google voice assistants. Using the mobile application, a user can lock or unlock doors remotely.

1.1.1.1.12 ***Discussion of threats***

From the discussion in Chapter 3 it was established that IoT devices generate a lot of data. Smart locks are just one additional IoT device responsible for such data. Although Yale is

known to produce strong mechanical locks, then adding smart features to the locks only means they will be prone to cyberattacks just like any internet-enabled device. Using the network module in locks such as the assure lock, enable the lock to provide many essential functionalities, such a remote locking of doors, getting messages on the state of the lock, some locks even managing to automatically lock the door once it detects the user has left the house. All these conveniences mean users might have to compromise their security. A large amount of data is collected and stored in the cloud. Reviewers argue that no server can guarantee safety of data since they are all prone to attacks. Yale though has given users the ability to demand their data be deleted from the servers.

Among the three locks being reviewed, August is the only company that has a very comprehensive privacy policy document, and clearly state what they collect, how they intend to use collected data. Although telling users of how they collect data, this does not make their locks any more secure. August locks provide the best smart features of the three manufacturers, but all these features make the lock even more prone to attacks. Some reviewers argue that the geolocation feature may allow attackers to pinpoint where the lock is located, and if the phone allowed to open the lock is stolen, it becomes easy for an intruder to get access to one's house. Using mobile app, quite a few personal information is collected, such as user information, location information, and device information. It is reported that many smart lock manufacturers, include Yale, are quick at releasing security patches when a security loophole is discovered.

Users who don't want their locks to integrate with the rest of other IoT devices in the HAN can just install the Bluetooth version of the lock. Reviewers claim that data traffic between the lock and the mobile app is encrypted, providing extra security for an attacker that has acquired access to the local network. Of course, with IoT the purpose is better integration of smart devices, hence the Schlage connect come equipped with Z-Wave, which allow it to connect to the IoT hub in a house and be able to communicate with other IoT devices. Remote management of this lock can only mean that data is transmitted to the internet, and if that happens then that data needs to be stored somewhere. It has already been brought out that

servers are also prone to attacks, storing sensitive data on them is a real security risk to users' privacy.

5.5.3 Smart Locks Findings

In this section the security concerns discussed in terms of vulnerabilities and threats identified in the data are summarised and combined from the two data sources. The aim is to identify specific concerns that needs to be taken into account in the development of guidelines for home owners regarding security concerns in smart homes, developed in Chapter 6.

The vulnerabilities and threat discussed in this section apply to the majority of smart locks, as long as they all support certain features that make them prone to cyberattacks.

5.5.3.1 *Threats identified from data*

The following threats were identified from manufacturer's documents as discussed in the previous section:

- Remote access of the locks;
- Access to geolocation data can reveal house location;
- Sharing of data with third-parties;
- Storage of user data on servers;

The following threats were identified from reviewers' documents as discussed in the previous section:

- Internet connectivity make locks prone to cyber-attacks;
- Large amount of data stored on servers in the cloud;
- Geolocation can allow attackers to pinpoint location of lock;
- Stolen connected phone can be used to unlock doors with geosensing feature;
- Lack of security updates opens the locks to attacks;
- Configuration settings may improve security based on encryption and connectivity.

These lists may be combined into a single list of threats posed by the use of smart speakers:

- Access to geolocation data can reveal house location;

- Sharing of data with third-parties;
- Storage of user data on servers put users' data at risk;
- Internet connectivity make locks prone to cyber-attacks;
- Geolocation can allow attackers to pinpoint location of lock;
- Stolen connected phone can be used to unlock doors with geosensing feature;
- Lack of security updates opens the locks to attacks;
- Locks can be controlled remotely;
- Large amount of data stored on servers in the cloud.
- Configuration settings may improve security based on encryption and connectivity.

These security concerns are compared with generic concerns in Chapter 6, and where appropriate, device specific guidelines are formulated for smart locks.

5.6 SMART FRIDGES

Smart fridges are Wi-Fi enable fridges equipped with an operating system and the ability to community over the internet and access cloud services. More specific characteristics of smart fridges is covered in Chapter 3.

5.6.1 Data collection for smart fridge

The data in Table 5-13 comes from a selected number of fridges based on the global market share. This section's data come from two sources, manufacturers' and reviewers' documents.

Table 5-13 Smart fridges data source

Manufacturer	Model	Motivation for selection	Manufacturer documents
S A M S U N G	Family Hub 3.0	Samsung is one of the world's leaders in consumer electronics. The following model is part of a family of smart fridges which are part of the Samsung Family Hub 2.0 range. The fridge has all the features that this study is investigating, such as the ability to connect to the internet, voice control using Bixby, the ability to control other smart things such as doorbells and smart locks by using Samsung SmartThings hub.	SAMSUNG (2019c) SAMSUNG (2019e) SAMSUNG (2019a)
L G	InstaView ThinQ	This model is selected because it falls under the smart fridge category, with all the features that the research is investigating. According to Hyde (2019), this model is listed as one of the best smart fridges in 2019.	LG (2019c)
G E	GE Profile Series	General Electric (GE) is one of the largest electric companies in the world which also has a division for home appliances. The model selected is a smart fridge with Wi-Fi connectivity and the ability to control it with Alexa. According to Hyde (2019), this the most family friendly smart fridge and it is ranked number one on the list of reviewed smart fridges.	GE (2019c) GE (2019b) GE (2019a)

5.6.2 Data presentation and coding

In this section, data from manufacturers and from reviewers are coded and presented in table format.

5.6.2.1 *Manufacturer documentations*

The information in Table 5-14 is representation of the data obtained from smart fridges manufacturers' documentations.

Table 5-14 Representation of manufacturers documents

Manufacturers	SAMSUNG			LG			GE		
Codes	YES	NO	NC	YES	NO	NC	YES	NO	NC
VULNERABILITY									
Acknowledges that the fridge can connect to the internet.	X			X			X		
Acknowledges that the smart application on the fridge allows a user to control other smart devices and appliances in the HAN.	X			X					
Acknowledges that the fridge can connect to servers in the cloud.	X			X					X
Acknowledges that the fridge has a built-in microphone for voice control.	X				X			X	
Acknowledges collecting data via the fridge.	X				X				X
Acknowledges that the same type of voice data collected through a smart TV is also applicable to a smart fridge.	X				X				X
Advises users to report stolen mobile devices with the controlling app on.			X			X	X		
THREAT									
Acknowledges that the fridge has a built-in microphone for voice control.	X				X			X	
Specifies that collected data is stored on servers for as long as it is needed by the company.			X			X	X		
Acknowledges that the transmission of collected data over the internet cannot be guaranteed to be 100%.			X			X	X		
Acknowledges sharing collected data with a third party.	X					X	X		

1.1.1.1.13 ***Discussion of vulnerabilities***

Samsung Family Hub range of fridges provide various smart functionalities that can make any house owner want to have one. The fridge comes with a large 21.5-inch display screen packed with a number of features. The fridge can connect to the internet and this allows various functionalities, such as controlling the fridge using voice commands, remote management and controlling of the fridge from the mobile application, getting status message from the fridge, being able to look inside the fridge remotely using the in-built cameras. One can even use the big screen on the fridge to control other smart devices in the house. All these functionalities require data to move between the fridge and the servers in the cloud. Samsung does not acknowledge storage of personal data on their servers, but they acknowledge sharing collected data with third parties. The fridge also comes with a built-in microphone which allows users to utter commands on Bixby. Samsung also acknowledges that the same way data is collected via their smart TVs is the same way voice data is also collected via the smart fridge.

The LG InstaView smart fridge is very similar to Samsung, with a big transparent OLED screen in front. The fridge provides all sort of smart features thanks to its internet connectivity. LG has incorporated Alexa voice assistant in the fridge's control system, meaning users can easily use voice commands to control the fridge. The internet connectivity also means the fridge can connect to the internet for various functions, controlling other LG appliances right from the fridge or searching for recipes on the internet. LG also makes use of the ThinQ mobile application to enable users to carry out remote functionalities or getting status messages from the fridge. Since the mobile app that is linked to the fridge can be used to remotely control the fridge, it means even in the wrong hands that can happen. LG advises users who might have lost their smart mobile devices to report this immediately so that the app can be disabled. When cloud services are used, devices are always sending and receiving data, but LG does not deny or admit that they collect data from their smart fridge and that this data is stored on servers in the cloud.

GE connected fridges have taken a different approach to that of Samsung and LG. The fridge does not have a big interactive touch screen for users, but the fridge has Wi-Fi connectivity

and is internet enabled. Using the internet, the fridge functionalities can be extended. For instance, voice control using Alexa on a smart speaker can be used to send command to the fridge. The mobile also allows the owner to remotely control or receive information on the status of the fridge. Very little information is provided by GE when it comes to smart features, which may be due to the fact the fridge does not have many inbuilt smart features like the competition.

1.1.1.1.14 ***Discussion of threats***

Samsung does not confirm if data is collected from their smart fridges or whether they store such data, but they acknowledge sharing data third party companies. There is also no mention if data is encrypted between smart fridge and the servers in the cloud. If any data is collected, there is no mention of how long they keep such data or what type of data it is. The fridge is equipped with all features that point to data collection, such as the microphone which able to receive voice commands, then Bixby needs to send these commands to the cloud services and wait for a response so that it can take action.

Not much information could be found about data collection that links straight to the smart fridge. There is no mention of the type of data collected or for what purpose it is collected, or how it is used or stored. They do however acknowledge the fridge having data collection features, such as the microphone which collect voice data, or the mobile application which gets data from the sensors in the fridge and send to the cloud for analysis. The mobile app is also able to remote control features of the smart fridge. LG does not elaborate how they protect user's data or how communication between the fridge and the servers in the cloud is protected.

GE, on the other hand, is clear when it comes to data collection, they agree to collect data and that all data collected is stored on servers in the cloud as long the company needs it. They also acknowledge that although they try to make the communication as secure as possible by encrypting the data, they argue that the consistency of the transmission can't be guaranteed.

5.6.2.2 ***Reviewer's documentations***

The data represented in Table 5-15 comes from reviewers' documents. The way the data is represented is explained in detail in Section 5.2.

Table 5-15 Representation of reviewer's documentations

Manufacturer	SAMSUNG					LG					GE			
Reviewer reference	R1 (Paul, 2017)	R2 (Heinzman, 2019)	R3 (Blecher, 2018)	R4 (Lloyd, 2018)	R5 (Bhartiya, 2017)	R1 (prnewswire.com, 2019)	R2 (Heinzman, 2019)	R3 (Ritchie, 2019)	R4 (ITweb, 2017)	R5 (Bhartiya, 2017)	R1 (Heinzman, 2019)	R2 (Nohe, 2017)	R3 (Elliot, 2019)	R4 (Sen, 2017)
VULNERABILITY														
Argues that a lack of security updates will compromise smart fridges as they get older.		Y ⁷⁰			Y ⁷¹					Y ⁷⁰	Y ⁷⁰			
Argues that the manufacturer does not warranty upgrade of their smart fridges when they get older.		Y ⁷²	N ⁷³		Y ⁷⁴					Y ⁷⁴				
Concurs that smart fridge has internet access.	Y ⁷⁵	Y ⁷⁶	Y ⁷⁷			Y ⁷⁸		Y ⁷⁹					Y ⁸⁰	

⁷⁰ The reviewer argues that a smart fridge that is not receiving updates will be vulnerable to cyberattacks.

⁷¹ The reviewer argues that lack of security updates will leave the device vulnerable to exploitations.

⁷² The reviewer argues that Samsung has the habit of not upgrading older version of their smart fridges. With the new Hub 2.0, Samsung warranty does not mention anything about the firmware being updated in the future. The warranty on the smart fridge only covers part replacement, there is no mention that after 5 or 10 years the firmware will continue to receive updates.

⁷³ The reviewer argues that, the fridge life span is around 14 years, although by that time the technology will be outdated, there is a likelihood that Samsung will continue to support the product.

⁷⁴ The reviewer argues that unlike company like tesla who have information on software update as the car get older, Samsung and LG do not mention anything on future upgrades.

⁷⁵ Agrees that smart features require internet connectivity for them to work.

⁷⁶ Agrees that Samsung family hub fridges do support smart features which work with internet connectivity.

⁷⁷ The reviewer conquers that the fridge has internet access.

⁷⁸ The reviewer agrees that LG smart fridge has internet connection for remote management.

⁷⁹ The reviewer concurs that the fridge smart features allow the fridge to connect to the internet.

⁸⁰ The reviewers agree that GE smart fridge supports internet connectivity which allows it to be controlled remotely using the mobile application. The user can also receive status messages from the different sensors installed in the fridge.

Manufacturer	SAMSUNG					LG					GE			
Admits that smart fridge can be used to control other smart devices.		Y ⁸¹	Y ⁸²					Y ⁸³						
Concurs that smart fridge can be controlled using voice commands.	Y ⁸⁴							Y ⁸⁵					Y ⁸⁶	
THREAT														
Argues that fridges OS or mobile apps may have security vulnerabilities.	Y ⁸⁷								Y ⁸⁸					Y ⁸⁹
Smart fridges are at risk of being compromised and used in a botnet.	Y ⁹⁰			Y ⁹¹						Y ⁹²		Y ⁹³		Y ⁹⁴
Argues that a fridge with an outdated software can compromise the whole network.		Y ⁹⁵			Y ⁹⁶		Y ⁹⁵				Y ⁹⁵			

⁸¹ The reviewer agrees that using the big screen, users can be able to control other smart devices such as cameras and door bells from the fridge.

⁸² The reviewer admits also that one can use the fridge to control other smart devices within a smart home.

⁸³ The InstaView fridge can be used to control another LG smart appliance.

⁸⁴ Samsung smart fridge come equipped with Bixby for voice control functionalities.

⁸⁵ The reviewer admits that Alexa comes built-in with the fridge to enable voice control of the fridge.

⁸⁶ The Wi-Fi connectivity on GE connected fridges expands its ability to be able to function with other devices, such as the integration work with Alexa and Google assistant for voice control.

⁸⁷ The reviewer argues that Samsung Tizen OS, which is used their smart TVs and smart fridges, inherited source codes from various Samsung projects, including the Bada OS. The majority of the code was poorly written and contains many security loopholes. It means devices using Tizen OS may also suffer from the same vulnerabilities.

⁸⁸ The reviewer argues that the LG mobile and the cloud applications were compromised by researchers in Israel in 2017, which gave them remote access to some LG products, including smart fridges.

⁸⁹ The reviewer argues that in an effort to push products to the market, manufacturers pay less attention to security, as a result IoT products, including smart fridges, may be shipped vulnerabilities in their software.

⁹⁰ The reviewer argues that due to the many vulnerability found in the OS used by Samsung, many of its smart appliances, such as smart fridges are at risk of being compromised and used in botnets to launch DDoS attacks.

⁹¹ The reviewer agrees that any smart devices can be attacked, but he also highlights that when the device is properly configured the risks of attacks can be minimized.

⁹² The reviewer concurs that a smart fridge with an outdated firmware can be compromised and used in botnet to launch DDoS attacks.

⁹³ The reviewer argues that in the 2016 Mirai malware attack, several IoT devices, including smart fridges, were compromised and used to mount DDoS attacks that brought down a number of big web sites.

⁹⁴ The reviewer concurs with most writers on the ability for a smart device, such as a fridge, to be used in a botnet.

⁹⁵ The reviewer argues that an outdated firmware of a smart IoT device, can compromise the security of the whole network.

⁹⁶ The reviewer agrees that an outdated firmware could be exploited exposing the device to cyberattacks.

Manufacturer	SAMSUNG					LG					GE			
Argues that all smart fridges are equipped with data-collecting algorithms.		Y ⁹⁷		Y ⁹⁸			Y ⁹⁷				Y ⁹⁷			N ⁹⁹
Argues that a smart fridge can be remotely controlled using an app.	Y ₁₀₀					Y ₁₀₁		Y ₁₀₂						

1.1.1.1.15 *Discussion of vulnerabilities*

Reviewers don't argue with the conveniences that smart fridges can add to one household. The ability to check inside your fridge from the shop if you forgot something, being able to view cooking shows right on the fridge with no need of an extra TV, getting statuses about expiry dates of products, or seeing who is at the front door without leaving your kitchen. These are all very useful features, but a blind eye can't be turned to the reality of security risks that these devices may bring along. Reviewers feel like manufacturers are not taking enough time to incorporate enough security into their devices. For instance, when it comes to the Tizen OS being used in smart devices, reviewers argue that the OS is full of vulnerabilities that intruders have been able to exploit in the past. The warranty section on Samsung smart fridges only cover hardware, what will happen five to ten years down the line? With no guarantee of software support when smart fridges get old, these appliances will be exposed to all kind of exploitation. The dangerous side of all this, is the privacy of data that such devices collect. With the ability for voice control, it means that Samsung must be collecting voice data and storing it somewhere. The fridge can be used to place orders online,

⁹⁷ The reviewer argues that since most smart fridges come equipped with data-collecting algorithms, when they don't get updates, privacy of data can become a real concern

⁹⁸ The reviewer argues that when a voice assistant, such as Bixby, is used, the voice commands travel to the servers on the internet where they are processed, and the results is returned to the device. The commands are store on servers but can also be deleted.

⁹⁹ The reviewer argues that although all IoT devices collect data, but the culprit is actually the user. She argues that easiness with which users are able to give up their personal data for some degree of convenience is alarming.

¹⁰⁰ The Samsung SmartThing app can allow the owner to interact with the fridge, such as checking the content of the fridge without opening it.

¹⁰¹ Argues that the LG ThinQ app can be used to remotely monitor or control the fridge.

¹⁰² The reviewer concurs that LG InstaView fridge can be remotely controlled using the ThinQ app on the phone.

meaning personal data will be transmitted. The fridge can also be used to control other smart appliances or devices. Having just one smart fridge that is compromised will be more than enough to compromise other IoT devices in the HAN.

Reviewers argue that all cloud-based services will require data to be sent and received from the cloud. The ThinQ application on mobile phone can be used to send commands to the fridge, but these commands are first sent to the servers and then to the fridge. When the fridge receives a voice command, the data is transmitted first to the cloud, after analysis, the fridge will receive a command to take action. Reviewers argue that all the data coming from the smart fridge end up being stored on servers. Reviewers also argue that LG does not provide any warranty that they will continue to provide software updates with time, as it has been argued by other reviewers, having an out of date firmware will expose the fridge to security exploits in time. Having a vulnerable smart fridge can put the rest of the IoT devices exposed to cyberattacks.

The internet connectivity ability of the fridge already put it at risk of being attacked. The Mirai malware that was used in DDoS attacks, is an indication that any smart fridge can vulnerable to cyberattacks. Little is mentioned on the firmware being used by GE or how often or quickly they update their smart fridges. From the data gathered, fridge can be exposed to exploit if a vulnerability has been found the updated is slow to come.

1.1.1.1.16 ***Discussion of threats***

A number of factors can put a smart fridge at risk of an attack. Reviewers argue that Samsung's own OS that is used on most of their smart devices, did not have a very good foundation. Because of that, researchers have been able to find countless vulnerabilities. The Mirai malware exploited vulnerabilities in IoT devices, including smart fridges. Thus, it is important that security patches are released regularly. Users can also contribute by checking that they are IoT device and appliances' firmware is up to date. Reviewers have raised an important point when it comes to Samsung giving a warranty that updates will be rolled out in the future even when new models are out. The life of a normal fridge is about 14 years, and in their warranty document, Samsung highlight things that they will replace after 5 or 10 years, yet there is no mention if they will continue to provide firmware updates for older

model and for how long. Unfortunately, a fridge can't just be replaced like a mobile phone. Reviewers argue that they will be a time when a number of IoT devices will be running old firmware and attackers will capitalise on this. The most important thing that will be put at risk is user's data and their privacy.

LG shares the same dilemma with Samsung when it comes to security updates. There is no software that can guarantee full protection. Reviewers argue that because of the proprietary technologies of most IoT devices, it becomes difficult for users to even install software to protect their devices. It then rests on the manufacturers to make sure this need is cared for. The LG's older version of ThinQ app was found to contain a vulnerability that allowed the researchers to compromise the application, and by doing so they gained remote access to another LG appliance. Although this vulnerability was fixed, it is a demonstration of how easy an attacker can gain access to these smart devices, causing havoc or stealing personal data from users. It has already been reported that only one compromised IoT device can put the whole HAN at risk, exposing all the other IoT devices to attacks.

No much is mentioned about GE smart fridges when it comes to data security, it might be due to the fact that the smart features the fridge offers are not as advanced as LG's or Samsung's. The fridge is still able to connect to the internet and collect data which alone is enough for the user to be aware of. GE agrees to collect data and store it in the cloud. It has been argued that no server can guarantee full protection of the data they store. GE argues that the communication between the smart fridge and the servers in the cloud is encrypted. This will provide a level of data protection and prevent data integrity breaches.

5.6.3 Smart Fridges Findings

In this section the security concerns discussed in terms of vulnerabilities and threats identified in the data are summarised and combined from the two data sources. The aim is to identify specific concerns that needs to be taken into account in the development of guidelines for home owners regarding security concerns in smart homes, developed in Chapter 6.

5.6.3.1 *Threats identified from data*

The following threats were identified from manufacturer's documents as discussed in the previous section:

- Sharing of data with third-parties;
- Presence of microphone;
- Remote management;
- Collecting of user's data;
- Indefinite storage of data in the cloud.
- Appliance might outlast the technology

The following threats were identified from reviewers' documents as discussed in the previous section:

- Poorly designed software;
- No warranty given on future software updates;
- Storage of user data in the cloud;
- Lack of proper checks for third-party apps;
- Transmission of unprotected data over the internet.

These lists may be combined into a single list of threats posed by the use of smart speakers:

- Sharing of data with third-parties;
- Presence of microphone;
- Remote management;
- Collection of user's data;
- Indefinite storage of data in the cloud;
- No warranty given on future software updates making appliances prone to future attacks
- Storage of user data in the cloud;
- Lack of proper checks for third-party apps;
- Transmission of unprotected data over the internet;

- Appliance might outlive the technology;
- Poorly designed software opens the device to attacks.

These security concerns are compared with generic concerns in Chapter 6, and where appropriate, device specific guidelines are formulated for smart fridges.

5.7 SMART GATEWAYS

A smart IoT gateway is device which allow multiple IoT devices to communicate in a HAN as described in Chapter 3. IoT gateways support multiple network protocols, including ZigBee, Z-Wave, and Wi-Fi. This allow gateways to interconnect devices from different vendors. Protocols such as ZigBee and Z-Wave can't connect to the internet, thus the gateway can connect these devices to the internet. IoT gateways come in different form factors as shown in Table 5-16, for instance, the SmartThings can be configured using an app and does not have a dedicated screen. The Google Nest hub and Amazon's Echo Show both are hybrid gateways, they both have a screen and have other features rather than just a smart gateway.

5.7.1 Data collection for smart gateways

The data sources for smart IoT gateways shown in Table 5-16 come from manufacturers' documents. From the hundreds of gateways available, the selected ones don't represent the whole market of smart gateways, but they are able to give a good understanding on the functionalities and security issues that may be found in gateways.

Table 5-16 Smart gateways data sources

Manufacturer	Model	Motivation for selection	Manufacturer documents
S A M S U N G	SmartThings Hub	These smart hubs are selected for this study based on their classifications from reviewers (Prospero, 2019a; Wetzel, 2019) as being among the best of smart hubs for 2019. From the lists of hubs reviewed, not all could be included for this study. The selection is balanced to include various manufacturers and form factors, as well as, feature supports.	SmartThings.com (2019)
G O O G L E	Nest hub max	For instance, the SmartThings hub does not have a screen where you can control them, but a user will need to use a mobile app to configure and control the hub. The Echo show and the Nest hubs both have built-in touch screens with control apps already installed, so a user can manage the hub using the touch screen.	Google (2019d) Google (2019c)
A M A Z O N	Echo show hub	The other feature the latter two have is a speaker, microphone, and camera. These extra features allow these hubs to be controlled using voice commands. The last selection criteria are the number of network protocol each can support, such as Wi-Fi, Bluetooth, Z-wave, and ZigBee.	Amazon (2019d) Amazon (2019b) Amazon (2019a)

5.7.2 Data presentation and coding

The gateways data represented in this section comes from the manufacturers’ and reviewers’ documents as discussed in Section 5.2. The data was analysed using content analysis as discussed in Section 5.2

5.7.2.1 *Manufacturer documentations*

Data represented in Table 5-17 comes from manufacturers’ documents, including manuals and privacy policy documents. The format of representing data in this table is explained in Section 5.2.

Table 5-17 Representation of manufacturers’ documentations

Manufacturers	Samsung			Google			Amazon		
Codes	YES	NO	NC	YES	NO	NC	YES	NO	NC
VULNERABILITY									
Acknowledges hub has ZigBee support.	X				X		X		
Acknowledges hub has Z-Wave support.	X				X				X
Acknowledges hub has Wi-Fi support.		X		X			X		
Acknowledges hub has Bluetooth support.	X			X			X		
Acknowledges that voice data is sent to the cloud.		X		X ¹⁰³			X		
Acknowledges collecting data from sensors.	X			X			X		
Specifies that users can turn off the mic and camera.		X		X			X		
Argues that voice recording only starts once the voice assistant pick up the key phrase.		X		X			X		

¹⁰³ Google argues that the voice audio is only sent to the cloud once the hub picks up the “Hey Google” key phrase. They argue also that users can delete all the voice queries the hub records.

Manufacturers	Samsung			Google			Amazon		
Codes	YES	NO	NC	YES	NO	NC	YES	NO	NC
Specifies that users can delete their audio recordings.		X		X			X		
Acknowledges collecting data about the device during setup process.	X			X ¹⁰⁴					
Acknowledges sharing of collected data with third parties.				X					
Acknowledges that the camera can be used to capture both videos and photos.		X		X			X		
Can be used to control other IoT devices.	X			X			X		
Specifies that the hub can be remotely managed.	X			X			X		
Manufacturer specifies what CPU the hub is using.		X			X		X ¹⁰⁵		
Manufacturer specifies how much RAM the hub is using.		X			X ¹⁰⁶			X	
Manufacturer specifies type of encryption used by the hub.					X		X ¹⁰⁷		
Allows installation of third-party apps.		X		X			X		
Manufacturer specifies the operating system being used by the hub.		X			X ¹⁰⁸			X	
Allow installation of third-party apps.		X		X			X		

¹⁰⁴ Collected data include device name, device type, and information about your home, including your address, ZIP code, and where the device is placed.

¹⁰⁵ Echo Show hub uses Intel Atom x5-Z8350 processor.

¹⁰⁶ Although this is not specified, the information can be obtained by checking the hardware specs on the hub.

¹⁰⁷ Although the manufacturer does not mention the type of encryption used, they do acknowledge that the encryption between the hub the cloud is encryption.

¹⁰⁸ None of the Google documentations specifies what OS the Nest Hub Max is using. The Android and IOS operating systems specified under specs on google store has to do with OS that support the Google Home app which is used to set up the hub.

Manufacturers	Samsung			Google			Amazon		
Codes	YES	NO	NC	YES	NO	NC	YES	NO	NC
Provides monitoring, control, and automation of smart devices via the mobile app.	X ¹⁰⁹			X ¹¹⁰			X ¹¹¹		
Can be controlled using a voice assistant.	X ¹¹²			X			X		
THREATS									
Acknowledges that hub uses face recognition using the built-in camera.		X		X					X
Acknowledges hub has a built-in microphone.		X ¹¹³		X ¹¹⁴			X		
Acknowledges built-in camera.		X		X ¹¹⁵			X		
Acknowledges that video footage is sent to the cloud.		X		X			X		
Connects sensor nodes and other IoT devices to the internet.	X			X			X		
Acknowledges storing collected data on their servers.			X	X ¹¹⁶			X ¹¹⁷		
Acknowledges that built-in camera is always recording.		X		X					X
Can control other IoT devices.	X ¹¹⁸			X			X		

¹⁰⁹ Using SmartThings app

¹¹⁰ The hub can be configured and controlled from a mobile app. There is both an Android and IOS version of the app.

¹¹¹ Using Alexa app

¹¹² Although the SmartThing hub does not have a microphone, but it has support voice command via Alexa or Google assistant through the mobile app, a smart speaker, or any other device that has the voice assistant installed.

¹¹³ This hub does not have scree, it relies on the mobile app for setup, control and monitoring. Since it has not camera or microphone, anything to do with these two sensors is not applicable to this hub.

¹¹⁴ Google argues that the microphone can be turned off.

¹¹⁵ Google argues that users can turn off the camera.

¹¹⁶ Google gives users options to delete both audio and video data that the hub collects.

¹¹⁷ The manufacturer argues that the data is stored in encrypted format.

¹¹⁸ SmartThings hub support a number of sensors, some made by Samsung and also sensors and other IoT devices from other manufacturers.

1.1.1.1.17 *Discussion of vulnerabilities*

The SmartThings gateway although not having a display screen, it is designed as a dedicated IoT gateway. It has support for more protocols than the Echo Show and Next hub. It has support for ZigBee, Z-Wave and Wi-Fi. These protocols allow the gateway to interconnect multiple IoT devices to communicate with one another. The gateway does not collect data, apart from the data collected via the mobile app during the setup. The SmartThing app allows a user to set up the hub and also configure other IoT devices. Since some IoT device can't connect directly to the internet, the gateway allows these devices to be controlled and monitored over the internet. All IoT devices are dependent on cloud services, the SmartThings hub also uploads data to servers on the internet. Internet connectivity also allows the hub to be controlled remotely. There is no mention on the OS the hub is using, or the amount of RAM installed, although this information can be retrieved from the app. SmartThing hub also has support for voice control, using this option, users can use a voice assistant on the app to send voice commands.

The Nest hub is a different category of gateways, it is more of a hybrid device. It has ten-inch screen and a speaker. It supports both Wi-Fi and Bluetooth. Using the hub, users can send voice commands to the hub to control compatible IoT devices. The hub has few built-in sensors which allow it to collect data. Google agrees to share some of the collected data with third parties, although they argue that they don't sell this data to advertisers. The hub has an operating system, although not specified by Google what it is using, there is also no mention on the hardware such as CPU or amount of RAM it is using. The hub can be configured using an app that can be downloaded from the Google Store for Android or Apple's app store for iOS devices. It must be noted that the mention of Android and iOS under the specifications' web page has to do with the software which is installed on mobile devices, and it has nothing to do with the OS running on the hub.

Amazon's Echo Show falls under the same form factor as the Next hub, it is also a hybrid device with other functionalities apart from its ability as a voice-controlled gateway. It supports voice commands using Alexa digital assistant. The hub has a camera as well as microphones. It has support for ZigBee, meaning it can be used to control and setup ZigBee

enable IoT devices. The hub works also with an app which allows users to set up the device. The device comes equipped with an Intel Atom x5-Z8350 processor, there no mention on the amount of RAM or the OS being used. Amazon does not mention if network traffic between the hub and servers in the cloud is encrypted, or if traffic between the hub and other IoT devices is encrypted.

1.1.1.1.18 ***Discussion of threats***

The SmartThing hub is playing the role as a central device in an IoT network, although it does not control other devices, it allows them to communicate despite different protocols they may be using. Unlike the other two hubs, SmartThings hub requires the use of app to configure it and control it. Using this app remote management is possible. The hub also has the highest number of devices it can control compared to the other two. As a smart home central controlling device, keeping the hub safe is vital. Samsung does not mention what encryption is used on the hub.

On the other hand, the Google Nest hub has sensors that may make it prone to attacks; features such as microphones and a camera. The microphones allow users to send voice commands to the gateway. The hub can connect to the internet, allowing it to send data to servers. Google acknowledges that they collect voice data from the device and save this on servers, Google claims though that users are able to delete this data. The camera on the device plays multiple roles, it can be used for video calls, it is a fully functional Nest security camera, and has facial tracking algorithm. As people passer-by or come closer to the device, it is able to do facial recognition, and when it detects the face, relevant information about the user is displayed on the screen. Data collected via sensors may end up stored on servers in the cloud. There is no mention what sort of encryption is employed to ensure transmitted data is kept safe.

Amazon's Echo show contain similar sensors to the Nest hub, have a built-in microphone and built-in camera. Data which is collected via these sensors is saved in the cloud. Unlike the Nest hub, Echo show can interact with many ZigBee IoT devices, from locks to motion detectors. All these devices may depend on the hub for security. It has also support remote

management using the app. Amazon does not specify what type of encryption is used in its hubs.

5.7.2.2 Reviewer's documentations

The representation of the reviewers' data in Table 5-18 is well in Section 5.2. The data in Table 5-18 comes from online reviews on the smart gateways. Of the thousands of reviews found online on this subject, only a few could be selected to give another perceptive on the security of the hubs.

Table 5-18 Representation of reviewers' documentations

Manufacturer	SmartThings				Google Hub Max					Echo Show		
Reviewer reference	R1 (Null, 2018)	R2 (Ludlow, 2019)	R3 (Prospero, 2019b)	R4 (Talos, 2018)	R1 (Crist, 2019c; Crist, 2019b)	R2 (Williams, 2019)	R3 (Gibbs, 2019)	R4 (Seifert, 2019)	R5 (Baron, 2019)	R1 (Chin, 2019)	R2 (Crist, 2019a)	R3 (Stegener, 2018)
VULNERABILITY												
Reviewer argues that the addition of camera on the hub is a concern.					Y ¹¹⁹		Y ¹²⁰		Y ¹²¹			
Drop-In feature in Echo show considered to be a privacy concern for users.										Y ¹²²		Y ¹²³

¹¹⁹ The reviewer argues that adding a video camera to the hub is a concern for many users.

¹²⁰ The reviewer argues that the addition of the camera introduces more worry about privacy.

¹²¹ The reviewer argues that although users can be aware the concerns posed by devices such the max, they are still reluctant to let go of such technology.

¹²² For the Echo show, the concern is with the drop pin feature, which allows someone to video call and start getting the video feed without the other party accepting the call. Although the feature is well intended for monitoring children or elderly parent, the reviewer find it to be a creepy feature.

¹²³ The reviewer argues that this feature add convenience for less privacy.

Manufacturer	SmartThings				Google Hub Max					Echo Show		
The hub has ability to control other IoT devices.	Y ¹²⁴	Y ¹²⁵								Y ¹²⁶		
Hub vulnerable to attacks.				Y ¹²⁷								
Firmware vulnerability allows intruders OS access.				Y ¹²⁸								
Hub configured using mobile app.		Y ¹²⁹	Y ¹³⁰									
Hub can be controlled using voice commands.		Y ¹³¹										
Reviewer specifies hub hardware.		Y ¹³²										
Reviewer claims the hub is running on a Linux.				Y ¹³³								
Ability by attackers to execute remote commands.				Y ¹³⁴								
Reviewer claims that the camera can record short videos and save them online.						Y ¹³⁵						

¹²⁴ SmartThings has support for both ZigBee and Z-Wave, this allow the hub to control a number of IoT devices that don't have Wi-Fi.

¹²⁵ Support for ZigBee and Z-Wave allows the hub to control a number of sensors from Samsung and third-party companies.

¹²⁶ The Echo show also dub as a ZigBee hub, able to control other IoT devices using voice commands. A user can also use it configure other IoT objects with not Wi-Fi connectivity.

¹²⁷ Reviewer argues that a number of vulnerabilities were discovered in SmartThing hub which allowed intruders to access other IoT devices such as unlocking smart locks, disabling motion detectors and more.

¹²⁸ Reviewer argues that vulnerabilities found in the firmware allowed attackers to issue OS commands.

¹²⁹ Using the SmartThings mobile app, users can control the hub and configure it. There is an Android and iOS versions of the app.

¹³⁰ Since the hub has no screen like the other two but makes use of the app on a mobile device. The reviewer claims that the purpose of the hub is not to control other smart IoT devices, rather to link them together.

¹³¹ Samsung does not have a smart speaker of its own, users can send voice command using the app on their mobile devices.

¹³² The reviewer claims that the hub has 256 Mb of RAM and 1 GHz CPU.

¹³³ Reviewer claims the OS used by the hub is based on a Linux kernel.

¹³⁴ The reviewer claims that with the vulnerabilities found, attackers could execute remote commands on the hub.

¹³⁵ The reviewer argues that the camera record short videos when it senses movement, and these videos are store online.

Manufacturer	SmartThings				Google Hub Max					Echo Show		
Audio recordings stored on servers.												Y ¹³⁶
Contractors used to listen to private conversations.					Y ¹³⁷						Y ¹³⁷	
No clarity in privacy policy on data access.					Y ¹³⁸						Y ¹³⁹	
Argues that a user can watch live feed from the hub from anywhere.						Y ¹⁴⁰		Y ¹⁴¹				
Hub may recognize users using their voices.							Y ¹⁴²					
Facial recognition data partially stored in the cloud.					Y ¹⁴³			Y ¹⁴⁴				
The reviewer argues that facial recognition data is not processed online.						Y ¹⁴⁵	Y ¹⁴⁶					
Reviewer claims that the Max give Google a wider window into its users' lives.					Y							
Trust of manufacturer is vital.							Y ¹⁴⁷					

¹³⁶ Reviewer argues that although Amazon gives users the option of deleting audio recordings, these are saved on servers in the cloud.

¹³⁷ Reviewer claims that both Amazon and Google used contractors to listen to recorded audio files collected via their devices. Both Amazon and Google claims though that only a small percentage of recorded voice data is given to expert to improve the service.

¹³⁸ Reviewer claims that manufacturer does not specify in their privacy policy about using its employee listening to recorded data.

¹³⁹ Reviewer claims that although Amazon and Google say they only use a small percentage of data to improve their services, there is no mention of such in the privacy policy document.

¹⁴⁰ By using the mobile app, a user can connect to the hub and watch a live feed from anywhere.

¹⁴¹ Confirms that users can stream the camera feed live to their mobile devices.

¹⁴² The reviewer claims that users can be recognized by the hub using their voices.

¹⁴³ Reviewer argues that when multiple users are involved, their face might be sent to Google to create a model, but the data is stored temporarily and then discarded.

¹⁴⁴ Argues that face recognition data which sent to the cloud by the mobile app is immediately deleted.

¹⁴⁵ The reviewer argues that Google claims the data used for facial recognition is stored locally on the device.,

¹⁴⁶ The reviewer claims facial recognition is done on the device itself and not in the cloud.

¹⁴⁷ The reviewer argues that for people to buy such a product, they will have to trust that the manufacturer will keep their privacy protected.

Manufacturer	SmartThings				Google Hub Max				Echo Show			
Collected data by home devices too much for one company.								Y ¹⁴⁸				
Reviewer claims the hub has up to 8 microphones.								Y ¹⁴⁹				
Users deserve a measure of privacy even with surveillance equipment installed.							Y ¹⁵⁰					
THREAT												
Facial recognition camera not wanted by buyers.					Y ¹⁵¹				Y ¹⁵²			
Device prone to cyberattacks.				Y ¹⁵³								Y ¹⁵⁴
Camera lacks a physical shutter.					Y ¹⁵⁵	Y ¹⁵⁶		Y ¹⁵⁷		Y ¹⁵⁸		

¹⁴⁸ The reviewer argues that the large amount of data collected through a device such as the max hub, can be too much for one company to have.

¹⁴⁹ Compared to the nest hub which has two microphones, the echo show has eight microphones which makes it good at listening to command even on top of music.

¹⁵⁰ The reviewer argues that despite people paying for equipment that can be using for surveillance purposes, they still expect a measure of privacy in their homes.

¹⁵¹ The reviewer argues that the facial recognition algorithm added in the Max hub is a feature many people don't want due to privacy concerns.

¹⁵² Reviewer argues that the max hub is a very problematic device due to its surveillance nurture.

¹⁵³ Vulnerabilities found in the firmware exposed the gateway to multiple remote attacks targeting connected devices.

¹⁵⁴ Reviewer argues that the device may be prone to cyberattacks and they can be turned into a wiretap.

¹⁵⁵ The reviewer argues that although Google added an electronic means to disable the camera, but users can't close the shutter with a physical cover when the camera is not in use. He argues that buyers might avoid buying the product due to privacy concerns, especially if such a device needs to be used a bedroom.

¹⁵⁶ Reviewer agrees that not having a physical cover for the camera can be a concern to users.

¹⁵⁷ Reviewer argues that lack of a physical shutter is a concern, but says Google guarantees the toggle switch to disable the camera is more than enough to prevent spoofing attacks.

¹⁵⁸ Reviewer argues that lack of a way to turn off the shutter maybe a concern for users who are afraid of snooping.

Manufacturer	SmartThings				Google Hub Max					Echo Show		
Camera on the hub is always scanning for faces.					Y ¹⁵⁹	Y ¹⁶⁰		Y ¹⁶¹	Y ¹⁶²			
Source codes of apps exposed on the internet.												
Claims vulnerable hub can expose sensitive data.				Y ¹⁶³								

1.1.1.1.19 *Discussion of vulnerabilities*

The SmartThings hub does not have any sensor built-in, but it provides interconnection to many IoT devices that support either ZigBee or Z-Wave. The hardware features of the smart hub can contribute to its security. For instance, the OS being used can be compromised by attacker if has security loopholes. It was discovered in 2018 that the second version SmartThings hub had close to twenty vulnerabilities that opened up the hub to a number of remote attacks. These vulnerabilities were all found in the OS or firmware. Although the loopholes found were fixed via security patches, it really demonstrates just how vulnerable the whole network can become due to a single compromised device. The worst part with smart hub is that, once it is compromised, all other IoT devices it provides network access to, are at risk of attacks.

The Nest hub is equipped with two types of sensors that raises a lot of privacy concerns, the video camera and the microphones. The dangers of smart devices using powerful microphones are well discussed under Section 5.4 on smart speakers. The addition of a video camera raises the concern levels of consumers. The video camera doubles also as a nest security camera, meaning a user can connect to this camera remotely using their mobile

¹⁵⁹ The reviewer claims that the camera on the Max hub is always scanning for faces in the room where it is placed, this is to allow it to automatically display certain info on the screen once it recognizes the user.

¹⁶⁰ Reviewer claims that the camera is always watching you 24/7.

¹⁶¹ Reviewer confirms that the camera is constantly trying to recognize faces.

¹⁶² Argues that the camera keeps scanning for passers-by to try and recognize them so that it can display customized information or play video messages left on the hub.

¹⁶³ Reviewer claims that IoT devices collect sensitive data, and this data is exposed to exploits when the hub has vulnerabilities.

phone. The reviewer claims that the camera records short videos when it senses movements and saves these recordings in the cloud. Although manufacturer may claim that stored data is secure, there are always chances that it may get leaked. For instance, the reviewer claims in one of the scandals involving data privacy, it was discovered that google allowed its workers or contractors to have access to private recorded data. Google claims that the data was used to train their systems. The issue though is that the company does not mention anything like that in their privacy documents. When it comes to the facial recognition feature, reviewers claim that the camera scanning faces of users may have security implications. Google claims that facial data is obtained once via the mobile app to create user profile, but it is deleted afterwards. All the facial recognition is done locally on the device and none of the captured videos is stored online.

Echo Show also suffers the same vulnerabilities that a device with a camera and microphone suffer from, in that it is also prone to these sensors being compromised. What is of concern is the data collected through these sensors and the fact that it ends up being stored online. One of the features on the Echo Show is called Drop-In, it allows a user to make video call to another camera enable Echo device, and the caller is able to get a live feed of the destination without the receiver answering the call. The feature is designed to monitor elderly parents by their children. Reviewers fear that this feature can make snooping much easier.

1.1.1.1.20 ***Discussion of threats***

The vulnerabilities discussed in the previous section exposed the SmartThings gateway to multiple attacks. Attackers could unlock doors, get access to camera feeds, control thermostats. Of course, users were advised to update their hubs as quick as possible. This really shows the dangers of poorly designed firmware. The reviewer argues that attackers could execute remotely OS commands. Due to the fact that the hub can connect too many sensors in a smart home and collect a large amount of data, a vulnerable gateway can expose users' sensitive data to exploits. The hub depends on the mobile app for configuration and remote management. Reviewers claim that several source code of various Samsung projects were exposed on GitLab, which is a public code repository accessible on the internet. It is

stipulated among the codes was found also source code of SmartThings hub, even source code pertaining to security features of the hub.

The always on camera on the Nest hub has left many reviewers concerned about privacy implications. One reviewer claims that such devices give manufacturers a wider view of our privacy. The facial recognition feature, although convenient for multiple users, but may expose users to serious privacy issues. Reviewers claim that the camera is always scanning for faces. Another feature on the device that all reviewers are concerned about is the lack of a physical shutter. If such a device is used in a bedroom, reviewers fear that if it is compromised, sensitive footage could be captured. Google claims that the camera can be disabled via software, the danger is that if an intruder is able to bypass that feature, nothing will stop them from gaining access to the camera.

The Echo Show has features that can put users at risks of attacks. The device has same sensor as the Nest hub, which put it under the same category of risks that may result from attackers gaining access to the video camera or microphones. The manufacturer does not specify if encryption is being used within the network or between the hub and the cloud. The hardware specification of the device can give an idea if such a device is capable of supporting encryption. In the case of the Echo Show, only the processor details is given, no amount of RAM or OS details are given.

5.7.3 Smart Hubs Findings

In this section, findings from data analysed from manufacturers and reviewers' document is presented. In this section the security concerns discussed in terms of vulnerabilities and threats identified in the data are summarised and combined from the two data sources. The aim is to identify specific concerns that needs to be taken into account in the development of guidelines for home owners regarding security concerns in smart homes, developed in Chapter 6.

5.7.3.1 *Threats identified from data*

The following security concerns were identified from manufacturers' documents as discussed in the previous section:

- Video camera always recording
- Microphones always listening
- Data stored in the cloud
- The camera always scanning for faces
- Remote access of devices via the gateway

The following security concerns were identified from reviewers' documents as discussed in the previous section:

- Vulnerabilities in firmware can give attackers access to other devices
- Facial recognition put users' privacy at risk
- Companies allowing its employees to listen to private recorded audio data
- No clarity on data access in private policy documents
- Lack of physical shutter on camera expose users to snooping
- Vulnerabilities of hub can expose users' data to exploitation
- Encryption policies not always stated

These lists can be combined into a single list of threats posed by the use of smart gateways:

- Video camera always recording
- Microphones always listening
- Data stored in the cloud
- The camera always scanning for faces
- Remote access of devices via the gateway
- Vulnerabilities in firmware can give attackers access to other devices
- Facial recognition put users' privacy at risk
- Companies allowing its employees to listen to private recorded audio data
- No clarity on data access in private policy documents
- Encryption policies not always stated
- Lack of physical shutter on camera expose users to snooping
- Vulnerabilities of the hub can expose users' data to exploitation

These security concerns are compared with generic concerns in Chapter 6, and where appropriate, device specific guidelines are formulated for smart TVs.

5.8 SUMMARY

The objective of this chapter is to fulfil the empirical objective of the study, by collecting data about security matters concerning smart appliances from manufacturers and reviewers. Since this is a deductive study the aim is to enhance the theoretical understanding of security threats in smart homes. Appliances and devices are selected based on availability and integration of specific sensors.

Before the presentation of the data, a discussion is provided on a strategy for data collection and presentation. Data from two sources are collected, presented and analysed in this study. These sources are documents from internet from manufacturers and reviewers of specific smart appliances and devices. For each device, two tables are developed to represent data from manufacturers and reviewers respectively. The data are analysed by creating codes in both tables. These codes further guide the discussions on the vulnerabilities and threats. Besides the discussions on the data, findings are presented as list of security concerns combined from the two data sources for each appliance or device to be used in the next chapter to develop guidelines.

A key conclusion of the data analysis and therefore of the chapter in support of the theoretical position of the study is the importance of data management policy and the communication thereof to users. A large number of codes concern what data is collected by sensors without the users' knowledge and what is done with the data. Information on which encryption methods used is relatively scarce. Another finding not clearly understood after the theoretical study, is the ability of other devices to support and take over the functionality of the gateway. This is specifically the case for smart speakers and more unexpectedly smart fridges. In the case of smart fridges, it creates a very specific vulnerability, since the lifespan of a fridge is much longer than that of the smart technology incorporated. If an unsuspected smart home owner buys a smart fridge today, would there still be support for the operating system, in terms of regular security updates, in ten years' time? A final observation not considered carefully enough is the strength or reach of the sensors and the fact that they are always on and always recording.

After reading all the documents in this study, the researcher is strongly under the impression of the lack of available knowledge for the everyday consumer on the invasion of privacy by the suppliers of these appliances and devices.

CHAPTER 6 GUIDELINE DEVELOPMENT

6.1 INTRODUCTION

The main purpose of this study is to identify security threats posed by smart home devices to unsuspecting homeowners in relation to their privacy in a home area network.

The aim of this chapter is to integrate the architecture perspective on security concerns developed in Chapter 3 and Chapter 4 with the empirical perspective developed in Chapter 5. The architecture perspective on security concerns was first developed intuitively in Chapter 3, based on an investigation of the nature of the components in an IoT network found in a smart home. After an investigation into network security focussing on IoT security, the same list of security concerns was refined and connected to specific literature, presented at the end of Chapter 4. This list was used to guide data collection.

Different manufacturers select different combinations of hardware components in their devices. The specific selection is often not known by the consumer. It is for example, not possible for the consumer to know which operating system is used by a specific appliance or how much memory is installed. But as indicated in Chapter 3 and Chapter 4, the choice of operating system and the hardware configuration of the sensor node is of extreme importance when it comes to the ability to protect the device.

Data management practices of manufacturers are most influential in the security and privacy of the home owners. This include capturing strategies encryption strategies, storage strategies and sharing policies. Although these vulnerabilities are inherent to the components, it is only when the reviewers' documents are studied that the extent of the danger becomes a reality.

Sometimes manufacturers provide enough technical information in their documentation, but the typical homeowner is not aware of the impact of specific components of the appliances

and data policies to better understand the specific vulnerabilities and threats for specific devices.

Technical reviewers of appliances also provide insights into the specific use of hardware components in a specific appliance. In other instances, the reviewers highlight specific security problems without supplying technical detail. In Chapter 5, documents compiled by reviewers of appliances were studied in order to gain an understanding of security concerns of a specific devices. A combined list of security concerns, for each category of devices, was developed from the two data sources in the findings section of Chapter 5.

This chapter presents a theoretical perspective on the findings of the manufacturer's and reviewer's documents presented in Chapter 5. The discussion is provided per appliance category and sensitive to the specific models investigated. The aim of each section is to reflect on the specific category of appliance in terms of the architecture while highlight specific insights for selected model. The end result is a list of security concerns grounded in the data of Chapter 5 and compatible with the architecture model-based concerns presented at the end of Chapter 4.

The presentation follows the same categories than Chapter 5, beginning with smart TVs (Section 6.3), followed by speakers (Section 6.4), locks (Section 6.5) and fridges (Section 6.6) with a separate reflection on gateways (Section 6.7). For each category a theoretical reflection is given in terms of the perception layer of the devices, followed by list of security concerns from the combined data sources developed in Chapter 5. A reflection is provided from the architectural layers to accommodate the concerns into the theoretical framework. Each section concludes with a set of guidelines for consumers to consider in selection and use of the type of appliance.

Following the argument that IoT devices share a basic architectural design, it is possible to compile set of generic guidelines for home owners of smart homes, independent from the specific device or appliance. Such a list restricts repetitions in the guidelines for specific appliances. The development of the generic guidelines is presented prior to the device guidelines and presented in Section 6.2.

6.2 GENERIC GUIDELINES FROM IOT ARCHITECTURE

It was shown in Chapter 3 that smart appliances are in a way a manifestation of a combination of heterogeneous components. The specific combination of sensors, sensor nodes and actuators that form the perception might differ from appliance to appliance, but from a security perspective, the underlying architecture of these devices are very similar and as argued in Chapter 4, each layer is prone to specific attacks whether it is in a washing machine or in a fridge. The architecture model developed by Vijayalakshmi and Arockiam (2016:34) is repeated here as Figure 6-1.

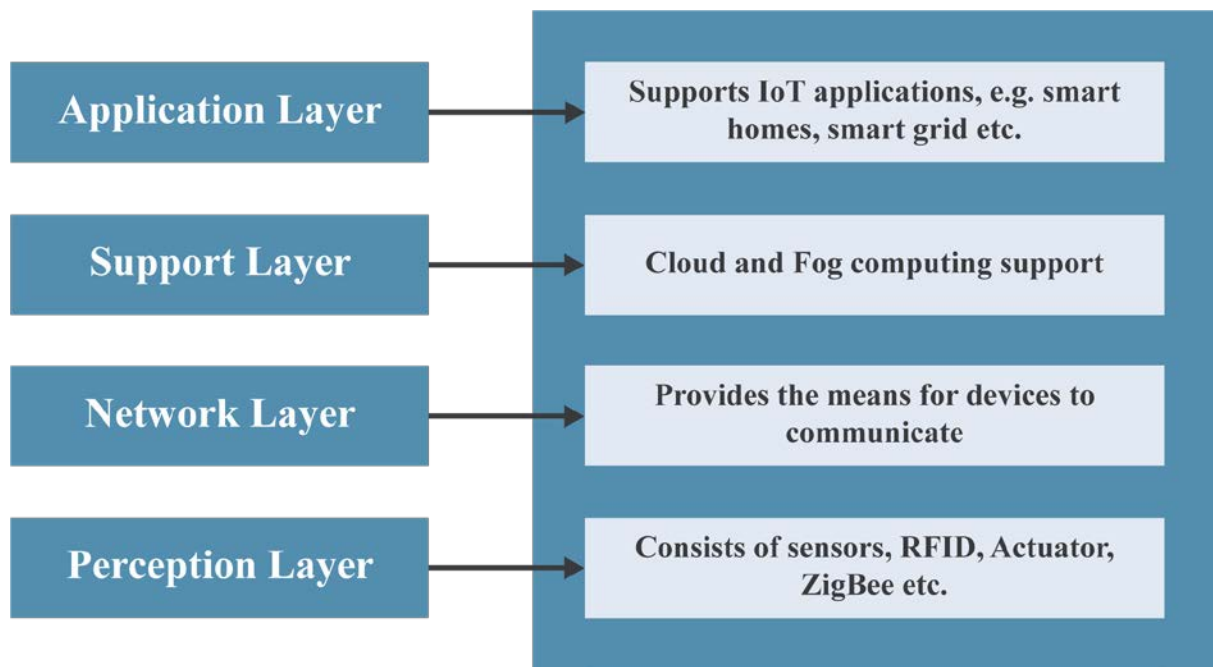


Figure 6-1 IoT architecture, adapted from (Ali et al., 2019)

Figure 6-1 IoT architecture, adapted from (Ali et al., 2019) is discussed in Chapter 3, in Section 3.8 in support of the initial list of security concerns which was refined and Chapter 4 and repeated here as Table 6-1.

Table 6-1 Security concerns of IoT networks from a theoretical perspective

Component	Security aspect
Application layer	
Appliance user interfaces	Smart appliances have specific settings which can be manipulated by the user. This is inherently an advantage and a threat as described for gateways. Lack of password control.
Gateway user interfaces	Again, a user interface creates opportunities for control of security settings but also vulnerabilities due to lack of knowledge by the user. Unauthorised access might be possible.
Mobile user interfaces	Mobile device applications pose many vulnerabilities to the home owner. The application programs to control the hub including the mobile application creates vulnerabilities since RFID can be simulated and other malicious command can be generated by potential attackers. Privacy is jeopardised.
<i>Application layer: Possible Attacks</i>	
• <i>DoS attack</i>: applications are also prone to DoS attacks. An intruder can use DoS attacks to destroy the availability of the application or the service it provides (Frustaci <i>et al.</i>, 2018:2484). • <i>Code injection</i>: with this type of attack, an intruder may inject malicious programming code into an IoT application, allowing him to exploit any vulnerabilities that the application may have (Frustaci <i>et al.</i>, 2018:2484). • <i>Malware attacks</i>: an intruder can target IoT application with malware, such as a Trojan horse or worms to steal data from the device (Ali <i>et al.</i>, 2019:462).	
Support Layer	
Connection from gateway to cloud	Connection to the internet creates vulnerabilities.
Cloud service provider.	Data storage by service provider also has vulnerabilities and might be subject to attacks.
<i>Support layer: Possible Attacks</i>	
• <i>Data security</i>: for data to remain secure in the cloud, it needs to be kept safe from security breaches (Ali <i>et al.</i>, 2019:460). Among these breaches are a breach of integrity, confidentiality, and availability (Silberschatz <i>et al.</i>, 2018:642). • <i>Virtualisation security</i>: different cloud vendors make use of a variety of virtualisation technologies, some of these are known to bypass network security measures. (Ali <i>et al.</i>, 2019:460) • <i>Tenant's security</i>: clouds vendors host files from multiple users. A single storage volume might contain files from other users. If security is not well implemented on these file servers, one user can steal data from another (Ali <i>et al.</i>, 2019:460).	
Network Layer	

Component	Security aspect
Connection of sensors to Gateway	Each sensor and its node use specific protocols to connect to the gateway. Wireless communication susceptible to eavesdropping.
Gateway Configuration	The ability of the user to manipulate security settings of gateways is both an advantage and vulnerability. It is an advantage when the user has enough knowledge of hardware, but when a user is not knowledgeable it becomes a vulnerability.
Gateway operating system	The sophistication of the operating system used by the gateway creates specific vulnerabilities.
Gateway hardware capacity	Aspects such as processor power and memory capacity influence the ability of the gateway to implement security measures and encryption.
Gateway mobile connection	The connection between the mobile phone and the gateway has inherent network vulnerabilities.
General connectivity threats	Network security threats can be viewed in terms of following four categories: interruption, interception, modification, and fabrication.
Network layer: Possible Attacks	
• <i>Denial of Service (DoS) and Distributed DoS (DDoS)</i>: Stewart <i>et al.</i> (2012:190) describe a DoS attack as “a resource consumption attack that has a primary goal of preventing legitimate activity on a victimised system”. The attacker can overload the network with traffic above its capacity making the network unavailable in the process (Ali <i>et al.</i>, 2019:460). • <i>Eavesdropping</i>: eavesdropping attacks are known to be passive in their nature. An intruder can simply listen to the traffic for the purpose of duplicating it (Stewart <i>et al.</i>, 2012:192). • <i>Routing attacks</i>: Routing attacks simply target the routing protocol being used by the router, or it targets the routing table (Anjum & Mouchtaris, 2007:10). Its aim is to modify the right routing path during the collection and forwarding process (Frustaci <i>et al.</i>, 2018:2484). • <i>Sybil Attacks</i>: a Sybil attack involves a node assuming multiple identities (Anjum & Mouchtaris, 2007:118), by impersonating other nodes or claiming a false identity. • <i>Replay attacks</i>: a replay attack involves capturing data being transmitted from one destination to another, and using this captured data to perform unauthorized actions (Bhaskar, 2008:26).	
Perception layer	
Sensors	
Image sensors: Camera and video camera	Images and videos are potentially captured without the knowledge of the homeowner and stored on the device or transmitted to the cloud.
Sound sensor: microphone	Sound clips are recorded, and potentially can be duplicated for remote voice activation of control devices.
Temperature / light sensors	Environmental conditions can be manipulated to achieve specific outcomes.
RFID tags	The tags of sensors can be simulated or duplicated to gain unauthorised access.
Sensor Nodes	

Component	Security aspect
Nodes and small computers	Due to size and cost factors the hardware capabilities are insufficient to support traditional operation systems and network protocols, leaving these devices vulnerable to attacks.
Sensor node operating systems	The appliances and hubs are loaded with operating systems to control the hardware. Due to size and cost considerations these operation systems are not on the same standard as PC operating systems in terms of security considerations. These smaller operating systems are vulnerable to code attacks and memory errors which may be exploited.
Smart electricity management	Vulnerabilities caused by service providers knowing the consumption patterns of home owners.
Smart meters	Communication between smart meter and utility supplier could jeopardise the privacy of the homeowner in that the communication could identify when the homeowner is not at home.
<i>Perception Layer: Possible Attacks</i>	
• <i>Sleep deprivation attacks</i>: IoT devices are known to have limited power source due to their reliance on battery (Miorandi <i>et al.</i>, 2012:1502). The attack causes the sensor node to stay awake draining the battery in the process (Khan & Salah, 2018:399). • <i>Malicious code injection</i>: this type of attack aims at compromising an IoT node by inserting malicious code into the node giving the intruder illegal access to the system (Ali <i>et al.</i>, 2019:460). • <i>RFID spoofing</i>: this type of attack targets RFID-enabled nodes by spoofing the signal and stealing the RFID tag. Once the tag is known, the attacker can send fake data using the original RFID tag, gaining full access to a system as a result (Ali <i>et al.</i>, 2019:460). • <i>Physical attacks</i>: an example of this is node tampering where an intruder might cause damage to items such as sensors, or by replacing a node or part of its hardware (Frustaci <i>et al.</i>, 2018:2484).	

Following from the argument that appliances has similar architectural structure a set of generic guidelines can be developed that holds true for most smart devices. These guidelines are grounded in Table 6-2 and presented and coded in Table 6-3 for later reference.

Table 6-2 General Guidelines for all IoT devices

Reference	Guideline
Application Layer	
G1: UserID	For each device in the smart home, be sure to understand the user interface, pay special attention to user access and authentication.
G2: AppConfig	For each device in the smart home, be sure to investigate which security settings can be configured by the user.

G4: MobileApp:	When using a mobile app to configure devices, be aware of vulnerabilities caused by outdated software and lack of updates.
G3: DeviceAccess	Restrict access to mobile devices used to control the gateway.
G4: MobileApp	Always set the mobile app to update automatically.
G5: Firmware	Ensure that smart device firmware is up to date.
Support Layer	
G6: CloudStorage	Be aware of service level agreements in terms of data protection, encryption and sharing of data.
G7: CloudConnect	Be aware of the security impact of the specific type of network use to upload data from the device to the cloud.
Network Layer	
G8: Protocols	Be aware of different types of networks used in smart homes and that the connection between devices may be insecure.
G9: HubConfig	Investigate which security and protocol settings can be controlled on the gateway to improve secure communication.
G10: HubOS	Investigate which OS is installed on a gateway, one used in current mobile phones and tablets are typically more secure than an unknown one.
G11: HubPower	Be aware of electricity options in terms of uninterrupted power supply of hub, since power cuts may be a form of attack.
G12 :HubAppLink	Be aware of the dangers concerning communication between mobile app and gateway for control. Investigate encryption provided and ensure it is activated.
Perception Layer	
G13:Sensors	Be aware of which sensors are installed in each device and which data they collect and importantly over what range they collect data.
G14:SensFail	Investigate the effects when a specific sensor fails in an appliance on its functionality and safety.
G15:AlwaysOn	Be aware of the time settings of data collection and the reach of the sensors in order to know when and where data is collected.
G16: :NodeOS	Investigate the OS used in appliance or host device in order to understand secure data storage and transfer from the specific device.
G17: :RFID	Be aware that individual devices have identification tags that may be copied in order to create insecure entry.

6.3 SECURITY CONCERNS OF SMART TVS

From a theoretical perspective it is important to note as presented in Chapter 3, Section 3.2 that smart TVs contains sensors for images and sound in the form of cameras and microphones. Manufacturers motivate users to connect the TVs to the internet to gain maximum functionality. When the smart television is connected to a gateway, all the guidelines presented in Table 6-2 applies to smart TVs.

From the manufacturer's documents security concerns as well as concerns from reviewers' documents were identified in Chapter 5. The combined list of security concerns is provided in Table 6-3. The table entries are grouped according to the architecture layers repeated in Figure 6-1. It should be noted that a specific concern originates from in a layer but influences all layers above that layer, for instance a sensor's data needs to be transmitted and stored which imply although the sensor is indicated in the perception layer, the network layer and the support layers are immediately indicated as well.

Table 6-3 Security concerns from data analysis for smart TVs

Security concerns from smart TV data
Application Layer
Operating systems used prone to attacks;
Presence of security loopholes in software;
Lack of security knowledge by device users;
Lack of stringent quality control of third-party software by manufacturers;
Lack of knowledge of privacy policy of users;
Different manufacturers have different OS with different features;
Support Layer

Storage of users' data on server in the cloud;
Sharing of data with third parties;
Possibility of the data falling into wrong hands;
Network Layer
Possibility of data transmission being intercepted;
Perception Layer
Collection of sensitive data;
Presence of microphone;

Although it is possible to link each of a concern to the generic guidelines presented in Table 6-2, concerns will inherently activate more than 1 guideline since these generic guidelines were compiled with the very nature of these devices in mind and should theoretically all apply to each device. When comparing the list of concerns with the list of generic guidelines, a number of concerns require additional more focused guidelines. Additional smart TV guidelines are proposed in Table 6-4.

Table 6-4 Additional smart TV guidelines

Guideline Ref	Additional Guideline	Code from data [Motivation for the additional guideline]
TV1: 3rdParty	Be aware that all additional app loaded on the TV may pose additional security concerns.	Lack of stringent quality control of third-party software by manufacturers.
TV2:UseNotrKnow	User should be aware that they need much more knowledge than anticipated in order to protect themselves.	Lack of security knowledge by device users.
TV3:Policy	Pay special attention to data collection and sharing in the policy documents of the specific manufacturer.	Lack of knowledge of privacy policy of users.
TV4: OSAware	Investigate the specific OS of a smart TV model. Different models of TVs use different operating systems, each with implications of security.	Different manufacturers have different OS with different features.

The next section presents the integration of literature and data findings for smart speakers.

6.4 SECURITY CONCERNS FOR SMART SPEAKERS

The perception layer of smart speakers comprises of very powerful microphones with long ranges. Specific voice commands are used to activate service, but in order to identify the commands the speaker should always “be listening”. This implies that data is gathered continuously. Data is stored on the cloud. It should be noted that smart speakers may act as input device for gateways, in which case the smart speaker becomes the input device for all smart devices. This increases the risk factor of these devices a thousand-fold.

Similar to the structure of the table in the previous section on smart TVs, Table 6-5 presents the summarised findings from the empirical data analysis of the two sources according to the architecture layers.

Table 6-5 Security concerns from data analysis for smart speakers

Security concerns from smart speaker data
Application Layer
Replication of user voice commands;
Intruders may use device to control gateway;
Support Layer
Data stored in cloud for long periods;
Network Layer
Built-in security lacking;
Perception Layer
Always on speaker;
Data is stored on the device itself.

When comparing the list of concerns with the list of generic guidelines, two concerns require additional guidelines. Additional smart speaker guidelines are proposed in Table 6-6.

Table 6-6 Specific smart speaker guidelines

Guideline Ref	Additional Guideline	Code from data [Motivation for the additional guideline]
Speaker1: DeleteData	User should delete old data from the device.	Data is stored on the device itself.
Speaker2: HighRiskDevice	Access to the device in a smart home should be considered as a risk and therefore users should know the range of their speakers.	Intruders may use device to control gateway.

The next section presents the integration of literature and data findings for smart locks.

6.5 SECURITY CONCERNS FOR SMART LOCKS

Smart locks as IoT objects, can collect a tremendous amount of data via the few sensors it has. For instance, it can sense if the door is locked or not, it can also when a person is approaching and automatically open for them using the geosensing feature. A compromised lock can expose the whole network to attacks, but even worse is the ability for an intruder to connect physical access to a house and plant a malware he could not use remotely.

Table 6-7 presents the summarised findings from the empirical data analysis of the two sources according to the architecture layers on smart locks.

Table 6-7 Security concerns from data analysis for smart locks

Security concerns from smart lock data
Application Layer
Stolen connected phone can be used to unlock doors with geosensing feature;
Lack of security updates opens the locks to attacks;

Support Layer
Sharing of data with third-parties;
Storage of user data on servers put users' data at risk;
Large amount of data stored on servers in the cloud;
Network Layer
Internet connectivity make locks prone to cyber-attacks;
Locks can be controlled remotely;
Perception Layer
Geolocation can allow attackers to pinpoint location of lock.

When comparing the list of concerns with the list of generic guidelines, a number of concerns require additional guidelines. Additional smart lock guidelines are proposed in Table 6-8.

Table 6-8 Specific smart lock guidelines

Guideline Ref	Additional Guideline	Code from data [Motivation for the additional guideline]
Lock 1: HighRiskDevice	Users should consider everything that can go wrong if security attach is experienced.	Stolen connected phone can be used to unlock doors with geosensing feature; Locks can be controlled remotely; Geolocation can allow attackers to pinpoint location of lock.
Lock2: Installation	Users should use qualified technician to install devices discuss security concerns with them,	Geolocation can allow attackers to pinpoint location of lock; Configuration settings may improve security based on encryption and connectivity.

The next section presents the integration of literature and data findings for smart fridges.

6.6 SECURITY CONCERNS FOR SMART FRIDGES

Today's smart fridges are equipped with a number of sensors on the perception layer. For instance, in the case of the Samsung hub smart fridge, it comes with microphones, cameras, motion sensors. These sensors render such appliances prone to exploitations. The ability for such appliances to connect to the internet and access cloud services means also an intruder could get remote access to the fridge. Apart from the fridge being used as an entry point to the network when it is compromised, an attacker can also create physical havoc.

Table 6-9 presents the summarised findings from the empirical data analysis of the two sources according to the architecture layers on smart fridges.

Table 6-9 Security concerns from data analysis for smart fridges

Security concerns from smart fridge data
Application Layer
Poorly designed software opens the device to attacks;
Lack of proper checks for third-party apps;
No warranty given on future software updates making appliances prone to future attacks;
Appliance might outlast the technology;
Support Layer
Transmission of unprotected data over the internet;
Sharing of data with third-parties;
Storage of user data in the cloud;
Indefinite storage of data in the cloud;
Network Layer

Remote management;
Similar concerns to gateways discussed in the next section;
Perception Layer
Collection of user's data;
Presence of microphone.

When comparing the list of concerns with the list of generic guidelines, a number of concerns require additional guidelines. Additional smart fridge guidelines are proposed in Table 6-10.

Table 6-10 Specific smart fridge guidelines

Guideline Ref	Additional Guideline	Code from data [Motivation for the additional guideline]
Fridge 1: HighRiskDevice	User Access is of greater importance since fridge can be used as gateway. Users need to be aware that their IoT fridge maybe not be able to detect that it has been affected by a malware, so extract precaution is needed to make sure they keep their appliances unaffected;	Similar concerns to gateways discussed in the next section Remote management.
Fridge2: Outlast	Users should be aware that the durable lifespan of the fridge itself is much longer than that of the technology. Support might not be available while the fridge is still working. This is especially a concern for security updates.	Appliance might outlast the technology
Fridge 3: FridgeAsGateway	When buying a fridge, a user should make himself/herself aware of all the security concerns of gateways.	Similar concerns to gateways discussed in the next section Appliance might outlive the technology

It must be noted that smart appliances may pose other physical threats as a result of them being compromised. For instance, if a smart washing machine could be compromised and be

operated remotely by an attacker, he can turn on an empty washing machine, maybe to the point of having water flooding the house; or an intruder may switch off a smart fridge resulting in food getting damaged; or a smart oven or stove might be left on for a long time risking the house being set on fire. So not only can an attacker compromise the privacy of the homeowners' data, but there exists real threat of damage to property or even fatality.

The next section presents the integration of literature and data findings for smart gateways.

6.7 SECURITY CONCERNS FOR SMART GATEWAYS

Smart gateways play a vital role in a smart home by being the network traffic coordinator within a HAN. a compromised gateway put all other devices that connect to it at risk of being exploited. Vulnerabilities in the software or firmware can expose users to data privacy dangers and the danger of having appliances such as stove being remotely controlled by an attacker. Table 6-11 presents the summarised findings from the empirical data analysis of the two sources according to the architecture layers on smart gateways.

Table 6-11 Security concerns from data analysis for smart gateways

Security concerns from gateway data
Application Layer
Vulnerabilities in firmware can give attackers access to other devices.
Vulnerabilities of the hub can expose users' data to exploitation.
Intruders may use device to control gateway.
Support Layer
Data stored in the cloud.
Companies allowing its employees to listen to private recorded audio data.

No clarity on data access in private policy documents.
Network Layer
Remote access of devices via the gateway.
Encryption policies not always stated.
Perception Layer
Video camera always recording.
Microphones always listening.
The camera always scanning for faces.
Lack of physical shutter on camera expose users to snooping.

When comparing the list of concerns with the list of generic guidelines, a number of concerns require additional guidelines. Additional smart gateway guidelines are proposed in Table 6-12.

Table 6-12 Specific gateway guidelines

Guideline Ref	Additional Guideline	Code from data [Motivation for the additional guideline]
Gateway1: HighRiskDevice	User Access is of great importance, since all other devices the home is connected to the gateway. The consequences of a possible attack concern every aspect of the network	Intruders may use device to control gateway. No clarity on data access in private policy documents
Gateway2: AlwaysOnSensors	Users need to be aware that the gateway has always watching camera and always listening microphones. This also implies that users should know the ranges of the sensors.	Video camera always recording. Microphones always listening. The camera always scanning for faces. Lack of physical shutter on camera expose users to snooping.
Gateway3: PrivacyMatters	Users should take responsibility to know what is recorded and what is done with the data.	Data stored in the cloud. Companies allowing its employees to listen to private recorded audio data.

Gateway4: HardwareOSMatters	Users should understand that secure network communication depends on hardware and OS capabilities of the gateway, as well as the continued support thereof in terms of updates.	Vulnerabilities in firmware can give attackers access to other devices. Encryption policies not always stated.
--------------------------------	---	---

This concludes the development of guidelines for the selected devices. The chapter is concluded with a summary.

6.8 SUMMARY

The aim of this chapter was to integrate the architecture perspective on security concerns developed in Chapter 3 and Chapter 4 with the empirical perspective developed in Chapter 5. The chapter starts by presenting generic guidelines for homeowners developed from the theoretical investigation presented in Chapter 3 and Chapter 4 on IoT components and network security.

Additional guidelines are then developed for specific appliances. These guidelines are derived from the empirical work carried out in Chapter 5 as an integral part of the device characteristics. From the identified threats, guidelines are developed to help homeowners with basic security practices. The guidelines focus on specific hardware components of these devices and also the way these devices and their manufacturers implement security and manipulate data.

The final conclusion for the study is provided in Chapter 7.

CHAPTER 7 CONCLUSION

7.1 INTRODUCTION

The main purpose of this study is to identify security threats posed by smart home devices to unsuspecting homeowners in relation to their privacy in a home area network.

The objective of this chapter is to summarise the research process and to communicate the findings of the study. The chapter is organised as follows, Section 7.2 provides a reflection on the objectives of the study, developed in Chapter 1. In Section 7.3, the main contribution is given in terms of the guidelines developed for home owners. The development of guidelines from the threats identified in Chapter 3, Chapter 4, and Chapter 5 is demonstrated in Chapter 6. The reflection on the research process is provided in section 7.4. This is organised according to the seven principles of conducting an interpretive study, focusing on how each of these were applied in this research. This evaluation also provides a reflection on the limitations to of study. By applying a manual data analysis method in the study, the researcher, being a computer scientist considers alternative approaches in Section 7.5 as future work resulting from this study. Section 7.6 provides a final summary for this chapter.

7.2 REFLECTION ON THE OBJECTIVES OF THE STUDY

The primary objective of the study is given in Chapter 1 as:

The primary objective of this study is to identify the security threats which smart home devices may pose to unsuspecting homeowners concerning their data privacy.

This primary objective is developed into theoretical and empirical sub-objectives as described below.

1. To investigate and justify the selection of a suitable research methodology for this study;
2. To demonstrate an understanding of smart devices in terms of hardware, software and network connectivity;
3. To demonstrate an understanding of security vulnerabilities leading to threats, posed by smart devices, in home area networks. This is done from a computer security literature perspective.

Empirical objectives

1. To collect data from manufacturers' technical documents and reviewers' documents on specific smart devices such as smart televisions, speakers, locks and fridges;
2. To compare and analyse the two data sources and literature in order to identify data privacy threats for these devices.
3. To develop guidelines for unsuspecting homeowners in relation to their privacy in home area networks, to consider when selecting smart devices.

The dissertation is summarised in terms of the stated objectives, starting with the theoretical objectives.

7.2.1 Reflection on theoretical objectives

The aim of the theoretical objectives is to create a shared understanding on the concepts used in the empirical study. Summaries of the literature chapters are provided to demonstrate the fulfilment of these objectives, starting with the objective on research methodology.

7.2.1.1 To investigate and justify the selection of a suitable research methodology for this study

This objective is achieved in Chapter 2 of this dissertation. Four research paradigms are discussed namely, positivism, interpretivism, critical social research, and design science research. Positivism involves the creation of hypotheses (Saunders, 2011:113); these hypotheses need to be proven by collecting data through repeatable experiments, from an objective perspective. This paradigm did not fit this research because the research was not

done from the ontological position of realism. The next considered paradigm was critical social theory. According to Leonardo (2004:11) the primary objective of this research paradigm is to provide emancipation. Since emancipation as part of the research process, is not the objective of this study, this paradigm was not adopted. The third research paradigm considered is design science research (DSR). DSR involves formulation and validation of models and theory on the phenomenon of a design, with the end goal being the creation of an artefact (Blessing & Chakrabarti, 2009:1). This paradigm does not fit the aim of this study; hence it was not adopted. The last paradigm evaluated was interpretivism. The goal of interpretivism is to understand different realities, this is achieved when researchers first gather data, then create theory to be tested by collecting more data. Interpretive research was selected as the best paradigm that fit this research. However, a deductive approach is followed in this study where the empirical study is done to better understand the phenomenon investigated from theory.

The research methods used is document research within a case study approach. Document research is selected because the sources of data used in the research all come from documents. Data was collected from two sources, manufacturers' and reviewers' documents. Content analysis was adopted as the data analysis method. Using content analysis, the collected data was coded into separate tables, one for manufacturers of each of the five categories of smart devices, and the other tables contains code from the reviewers' documents on the same smart devices' categories. The principles of Klein and Myers (1999:69) guided the research as discussed in Chapter 2. These principles are repeated in Section 7.4 to aid the evaluation of the study.

7.2.1.2 To demonstrate an understanding of smart devices in terms of hardware, software and network connectivity

This objective is achieved in Chapter 3 of this dissertation. The architectural model for IoT devices repeated in Figure 7-1. It is the position of the researcher that different type of smart devices has common features at the perception layer, for instance, they come equipped with a variety of sensors for data collection. On the network layer level, most IoT devices support some or other form of network. For instance, some IoT objects can support only Z-Wave,

while others can support only ZigBee, others Bluetooth or Wi-Fi only. Thus, for such devices to communicate, a gateway is needed. A number of gateways are considered in the discussion, but they all have one common function, and that is to connect all IoT devices to the same network in order to communicate. On the support layer, it is shown that smart gateways enable IoT devices to communicate with cloud services by providing them with internet connectivity. On the application layer level, it is shown that all IoT devices have some form of software installed. All devices have a firmware, for the majority this is a Linux based OS which controls the hardware of the device, such as RAM, CPU and others.

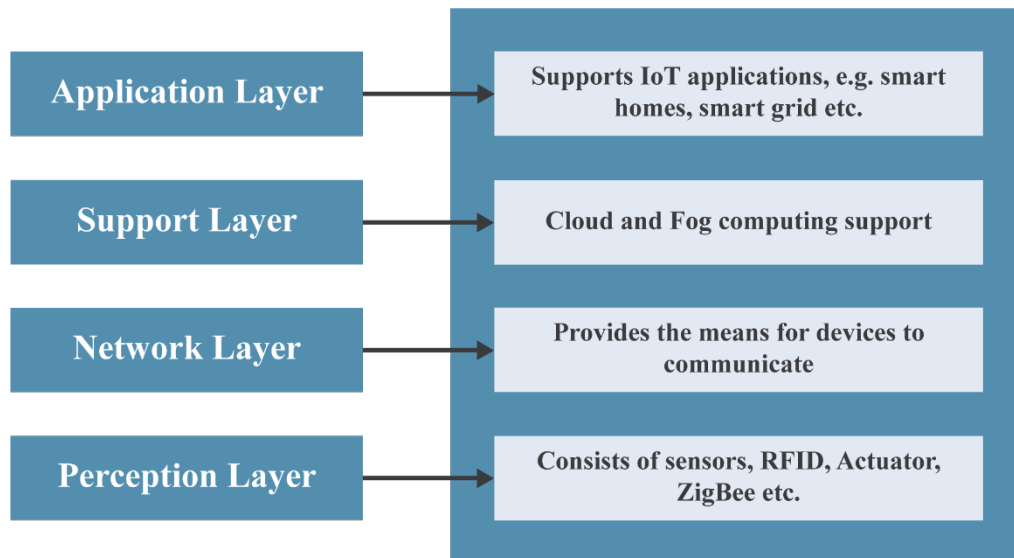


Figure 7-1 IoT architecture, adapted from (Ali et al., 2019)

7.2.1.3 *To demonstrate an understanding of security threats posed by smart devices to data privacy in home area networks from a computer security literature perspective*

This objective is achieved in Chapter 4 of this dissertation. It is shown that vulnerabilities can be exploited by an intruder and this may lead to an attack. It is found that due to the lack of standards concerning IoT, many manufacturers seem to implement their own versions of operating systems or developing their own software. Many IoT technologies are still closed source, and this makes it difficult at times to check for all vulnerabilities that are found in the source codes. Manufacturers tend to rush products to the market with little security or no security implemented at all. The heterogeneity of IoT technologies also creates many loop

holes that attackers are able to explore. It is argued that, the hardware limitations of IoT devices and appliances makes it difficult to implement traditional security measures such as encryption. Due to the closed nature of most smart devices, it is impossible for users to install any software to monitor the security of the device. For instance, if a smart appliance is affected with a malware, it is almost impossible for the owner to notice this. The many vulnerabilities that exist in these devices, allow intruders to control these devices resulting in stealing users' data, manipulating the sensors or compromising the entire system by means of DDoS attacks. In Table 7-1, security concerns are presented according to the four-layer structure of IoT. At each layer, components are identified with their corresponding security concerns.

Table 7-1 Security concerns of IoT networks from a theoretical perspective

Component	Security aspect
Application layer	
Appliance user interfaces	Smart appliances have specific settings which can be manipulated by the user. This is inherently an advantage and a threat as described for gateways. Lack of password control.
Gateway user interfaces	Again, a user interface creates opportunities for control of security settings but also vulnerabilities due to lack of knowledge by the user. Unauthorised access might be possible.
Mobile user interfaces	Mobile device applications pose many vulnerabilities to the home owner. The application programs to control the hub including the mobile application creates vulnerabilities since RFID can be simulated and other malicious command can be generated by potential attackers. Privacy is jeopardised.
<i>Application layer: Possible Attacks</i>	
• <i>DoS attack</i>: applications are also prone to DoS attacks. An intruder can use DoS attacks to destroy the availability of the application or the service it provides (Frustaci <i>et al.</i>, 2018:2484). • <i>Code injection</i>: with this type of attack, an intruder may inject malicious programming code into an IoT application, allowing him to exploit any vulnerabilities that the application may have (Frustaci <i>et al.</i>, 2018:2484). • <i>Malware attacks</i>: an intruder can target IoT application with malware, such as a Trojan horse or worms to steal data from the device (Ali <i>et al.</i>, 2019:462).	
Support Layer	

Component	Security aspect
Connection from gateway to cloud	Connection to the internet creates vulnerabilities.
Cloud service provider.	Data storage by service provider also has vulnerabilities and might be subject to attacks.
<i>Support layer: Possible Attacks</i>	
- Data security: for data to remain secure in the cloud, it needs to be kept safe from security breaches (Ali et al., 2019:460). Among these breaches are a breach of integrity, confidentiality, and availability (Silberschatz et al., 2018:642). - Virtualisation security: different cloud vendors make use of a variety of virtualisation technologies, some of these are known to bypass network security measures. (Ali et al., 2019:460) - Tenant's security: clouds vendors host files from multiple users. A single storage volume might contain files from other users. If security is not well implemented on these file servers, one user can steal data from another (Ali et al., 2019:460).	
Network Layer	
Connection of sensors to Gateway	Each sensor and its node use specific protocols to connect to the gateway. Wireless communication susceptible to eavesdropping.
Gateway Configuration	The ability of the user to manipulate security settings of gateways is both an advantage and vulnerability. It is an advantage when the user has enough knowledge of hardware, but when a user is not knowledgeable it becomes a vulnerability.
Gateway operating system	The sophistication of the operating system used by the gateway creates specific vulnerabilities.
Gateway hardware capacity	Aspects such as processor power and memory capacity influence the ability of the gateway to implement security measures and encryption.
Gateway mobile connection	The connection between the mobile phone and the gateway has inherent network vulnerabilities.
General connectivity threats	Network security threats can be viewed in terms of following four categories: interruption, interception, modification, and fabrication.
<i>Network layer: Possible Attacks</i>	
- Denial of Service (DoS) and Distributed DoS (DDoS): Stewart et al. (2012:190) describe a DoS attack as “a resource consumption attack that has a primary goal of preventing legitimate activity on a victimised system”. The attacker can overload the network with traffic above its capacity making the network unavailable in the process (Ali et al., 2019:460). - Eavesdropping: eavesdropping attacks are known to be passive in their nature. An intruder can simply listen to the traffic for the purpose of duplicating it (Stewart et al., 2012:192). - Routing attacks: Routing attacks simply target the routing protocol being used by the router, or it targets the routing table (Anjum & Mouchtaris, 2007:10). Its aim is to modify the right routing path during the collection and forwarding process (Frustaci et al., 2018:2484). - Sybil Attacks: a Sybil attack involves a node assuming multiple identities (Anjum & Mouchtaris, 2007:118), by impersonating other nodes or claiming a false identity.	

Component	Security aspect
Replay attacks: a replay attack involves capturing data being transmitted from one destination to another, and using this captured data to perform unauthorized actions (Bhaskar, 2008:26).	
Perception layer	
Sensors	
Image sensors: Camera and video camera	Images and videos are potentially captured without the knowledge of the homeowner and stored on the device or transmitted to the cloud.
Sound sensor: microphone	Sound clips are recorded, and potentially can be duplicated for remote voice activation of control devices.
Temperature / light sensors	Environmental conditions can be manipulated to achieve specific outcomes.
RFID tags	The tags of sensors can be simulated or duplicated to gain unauthorised access.
Sensor Nodes	
Nodes and small computers	Due to size and cost factors the hardware capabilities are insufficient to support traditional operation systems and network protocols, leaving these devices vulnerable to attacks.
Sensor node operating systems	The appliances and hubs are loaded with operating systems to control the hardware. Due to size and cost considerations these operation systems are not on the same standard as PC operating systems in terms of security considerations. These smaller operating systems are vulnerable to code attacks and memory errors which may be exploited.
Smart electricity management	Vulnerabilities caused by service providers knowing the consumption patterns of home owners.
Smart meters	Communication between smart meter and utility supplier could jeopardise the privacy of the homeowner in that the communication could identify when the homeowner is not at home.
<i>Perception Layer: Possible Attacks</i>	
- Sleep deprivation attacks: IoT devices are known to have limited power source due to their reliance on battery (Miorandi et al., 2012:1502). The attack causes the sensor node to stay awake draining the battery in the process (Khan & Salah, 2018:399). - Malicious code injection: this type of attack aims at compromising an IoT node by inserting malicious code into the node giving the intruder illegal access to the system (Ali et al., 2019:460). - RFID spoofing: this type of attack targets RFID-enabled nodes by spoofing the signal and stealing the RFID tag. Once the tag is known, the attacker can send fake data using the original RFID tag, gaining full access to a system as a result (Ali et al., 2019:460). - Physical attacks: an example of this is node tampering where an intruder might cause damage to items such as sensors, or by replacing a node or part of its hardware (Frustaci et al., 2018:2484).	

This table represents the theoretical position taken in the study. The empirical work is done to broaden the understanding of smart home security as phenomenon. It is the position of the study that smart devices have similar security concerns due to their inherent architecture. However, manufacturers select specific hardware components leading to particular concerns and adopt specific data management policies affecting the privacy of the home owners.

7.2.2 Reflection on empirical objectives

The empirical objectives of the study are presented in this section to aid the summary of the research conducted. The empirical report is provided in Chapter 5 and reflection on the theoretical position in terms of the findings is done in Chapter 6.

7.2.2.1 To collect data from manufacturers' technical documents and reviewers' documents on specific smart devices such as smart televisions, speakers, locks and fridges

The data collection and analysis strategy for this first data source is detailed in Section 5.2. It summarises the process followed to collect data and justify the selection of specific documents for this study: In total around 30 manufacturers' documents were studied with regard to 15 specific models of devices and about 30 reviewers' documents were analysed. For manufacturers, data was collected from devices' technical manuals, from privacy policy documents, and other company websites pages that were relevant to the data collection process. A large number of reviews were evaluated for each device category, and from these, the best reviews that provide relevant information to the study are used in the study. The purpose of collecting this data was to understand the various components that are used in building smart devices, and the roles these components play in the security of the devices, as well as manufacturer's policies on managing the large amount of data collected.

7.2.2.2 To compare and analyse the two data sources and literature in order to identify data privacy threats for these devices.

This objective is accomplished in Chapter 5. Data was collected from manufacturers' and reviewers' documents. The data was analysed using content analysis to identify the security concerns in general. Since this is a deducted interpretive study where the empirical study was done in order to enhance the understanding from the theoretical perspectives, the identified

threats are not representative of all the threats but rather those that serves the purposes of the empirical study. Table 7-2 provide the summary of the threats identified in enhancement of the theoretical perspective repeated in Table 7-1.

Table 7-2 Combined security threats from data

Application layer	Support Layer	Network Layer	Perception Layer
Smart Television			
• Operating systems used prone to attacks; • Presence of security loopholes in software; • Lack of security knowledge by device users; • Lack of stringent quality control of third-party software by manufacturers; • Lack of knowledge of privacy policy of users; • Different manufacturers have different OS with different features;	• Storage of users' data on server in the cloud; • Sharing of data with third parties; • Possibility of the data falling into wrong hands;	• Possibility of data transmission being intercepted;	• Collection of sensitive data; • Presence of microphone;
Smart speaker			
• Replication of user voice commands; • Intruders may use device to control gateway;	• Data stored in cloud for long periods;	• Built-in security lacking;	• Always on speaker; • Data is stored on the device itself.
Smart Lock			
• Lack of security updates opens the locks to attacks;	• Sharing of data with third-parties; • Sharing of data with third-parties; • Large amount of data stored on servers in the cloud.	• Internet connectivity make locks prone to cyber-attacks; • Locks can be controlled remotely;	• Geolocation can allow attackers to pinpoint location of lock.

Smart Fridge			
• Poorly designed software opens the device to attacks; • Lack of proper checks for third-party apps; • No warranty given on future software updates making appliances prone to future attacks; • Appliance might outlast the technology;	• Transmission of unprotected data over the internet; • Sharing of data with third-parties; • Storage of user data in the cloud; • Indefinite storage of data in the cloud;	• Remote management; • Similar concerns to gateways discussed in the next section;	• Collection of user's data; • Presence of microphone.
Smart Gateway			
• Vulnerabilities in firmware can give attackers access to other devices; • Vulnerabilities of the hub can expose users' data to exploitation; • Vulnerabilities of the hub can expose users' data to exploitation.	• Data stored in the cloud; • Companies allowing its employees to listen to private recorded audio data; • No clarity on data access in private policy documents.	• Remote access of devices via the gateway; • Encryption policies not always stated.	• Video camera always recording; • Microphones always listening; • The camera always scanning for faces; • Lack of physical shutter on camera expose users to snooping.

When this table is read column by column, similarities between the devices in terms of security concerns may be identified.

In terms of the perception layer it is alarming from a security concern that the devices are always recording data from their surroundings. The network layer concerns are mainly focussed on the lack of encryption and general interception concerns, supporting of the theoretical findings of Chapter 4. Remote access creates an inherent concern.

From the support layer column if read from top to bottom, it is easy to see what the theme is. All these devices can collect data in one form or another; they all transmit the data to cloud servers for storage; the data may be stored indefinitely; it can be shared with others without the owners' consent. In terms of application concerns, general software concerns are

identified as well operating system concern. The safeguarding of operating systems is dependent on hardware capability and commitment of suppliers in terms security updates.

The third empirical guideline: To develop guidelines for unsuspecting homeowners in relation to their privacy in home area networks, to consider when selecting smart devices represents the main contribution of the study

7.3 CONTRIBUTION: GUIDELINES FOR HOME OWNERS

The position of the study is that the empirical study is in support of theoretical investigation. The theoretical investigation summarised in Table 7-1 is used in Chapter 6 to derive generic guidelines based on the architecture of IoT devices and repeated in Table 7-3. These guidelines hold true for all smart devices which can be described in terms of the architecture or a subset of layers of it.

Table 7-3 Generic guidelines form literature

Reference	Guideline
Application Layer	
G1: UserID	For each device in the smart home, be sure to understand the user interface, pay special attention to user access and authentication.
G2: AppConfig	For each device in the smart home, be sure to investigate which security settings can be configured by the user.
G4: MobileApp:	When using a mobile app to configure devices, be aware of vulnerabilities caused by outdated software and lack of updates.
G3: DeviceAccess	Restrict access to mobile devices used to control the gateway.
G4: MobileApp	Always set the mobile app to update automatically.
G5: Firmware	Ensure that smart device firmware is up to date.
Support Layer	
G6: CloudStorage	Be aware of service level agreements in terms of data protection, encryption and sharing of data.

G7: CloudConnect	Be aware of the security impact of the specific type of network use to upload data from the device to the cloud.
Network Layer	
G8: Protocols	Be aware of different types of networks used in smart homes and that the connection between devices may be insecure.
G9: HubConfig	Investigate which security and protocol settings can be controlled on the gateway to improve secure communication.
G10: HubOS	Investigate which OS is installed on a gateway, one used in current mobile phones and tablets are typically more secure than an unknown one.
G11: HubPower	Be aware of electricity options in terms of uninterrupted power supply of hub, since power cuts may be a form of attack.
G12 :HubAppLink	Be aware of the dangers concerning communication between mobile app and gateway for control. Investigate encryption provided and ensure it is activated.
Perception Layer	
G13:Sensors	Be aware of which sensors are installed in each device and which data they collect and importantly over what range they collect data.
G14:SensFail	Investigate the effects when a specific sensor fails in an appliance on its functionality and safety.
G15:AlwaysOn	Be aware of the time settings of data collection and the reach of the sensors in order to know when and where data is collected.
G16: :NodeOS	Investigate the OS used in appliance or host device in order to understand secure data storage and transfer from the specific device.
G17: :RFID	Be aware that individual devices have identification tags that may be copied in order to create insecure entry.

However, it is clear from the empirical data that data handling in terms of privacy is an important consideration. Additional device specific guidelines are developed in Chapter 6 and summarised here as Table 7-4.

Table 7-4 Additional device specific guidelines from empirical study

Guideline Ref	Additional Guideline
Television	
TV1: 3rdParty	Be aware that all additional app loaded on the TV may pose additional security concerns.

TV2:UseNotrKnow	User should be aware that they need much more knowledge than anticipated in order to protect themselves.
TV3:Policy	Pay special attention to data collection and sharing in the policy documents of the specific manufacturer.
TV4: OSAware	Investigate the specific OS of a smart TV model. Different models of TVs use different operating systems, each with implications of security.
Smart Speakers	
Speaker1: DeleteData	User should delete old data from the device.
Speaker2: HighRiskDevice	Access to the device in a smart home should be considered as a risk and therefore users should know the range of their speakers.
Smart Locks	
Lock 1: HighRiskDevice	Users should consider everything that can go wrong if security attach is experienced.
Lock2: Installation	Users should use qualified technician to install devices discuss security concerns with them,
Smart Fridges	
Fridge 1: HighRiskDevice	User Access is of greater importance since fridge can be used as gateway. Users need to be aware that their IoT fridge maybe not be able to detect that it has been affected by a malware, so extract precaution is needed to make sure they keep their appliances unaffected;
Fridge2: Outlast	Users should be aware that the durable lifespan of the fridge itself is much longer than that of the technology. Support might not be available while the fridge is still working. This is especially a concern for security updates.
Fridge 3: FridgeAsGatway	When buying a fridge, a user should make himself/herself aware of all the security concerns of gateways.
Smart gateways	
Gateway1: HighRiskDevice	User Access is of great importance, since all other devices the home is connected to the gateway. The consequences of a possible attack concern every aspect of the network
Gateway2: AlwaysOnSensors	Users need to be aware that the gateway has always watching camera and always listening microphones. This also implies that users should know the ranges of the sensors.
Gateway3: PrivacyMatters	Users should take responsibility to know what is recorded and what is done with the data.
Gateway4: HardwareOSMatters	Users should understand that secure network communication depends on hardware and OS capabilities of the gateway, as well as the continued support thereof in terms of updates.

Once again, similarities can be observed in these guidelines. From comparing all the five categories of devices, it can be seen that central themes are:

- I. Access control to device management*
- II. Risk to data privacy*
- III. Lack of user knowledge.*

An evaluation of the research project is provided in the following section

7.4 EVALUATION OF RESEARCH

In this section, we look at how the seven principles of conducting an interpretive research by Klein and Myers (1999:69) were applied in this research.

7.4.1 Principles for interpretive case work

With every research project, there are guidelines that direct the researcher in the way he/she should carry out his/her research. These guidelines help in making sure certain standards are followed. In this section, seven guidelines or principles of conducting an interpretive case study research are discussed.

- I. The fundamental principle of hermeneutics*

The hermeneutics circle helps in understanding the whole by looking at the parts. In this research the objective is to identify threat to data privacy that smart devices may pose in a HAN. This objective can be referred as the whole, and to reach this objective the parts need to be analysed first. This was accomplished by looking at the security of five categories of smart devices, and for each category, components vital to the devices were analysed using IoT layered structure to see how each component contributes to the security of the device, and how each device contributes to the security of the HAN. The hermeneutic circle could also be applied to smart gateways in the way they can affect the security of the network. For instance,

as a central device, a vulnerable gateway can compromise the security of all devices in the HAN as a whole.

II. The principle of contextualization

This principle applies to this research. Through the analysis of many documentations on privacy policies of the various appliances under study, it is important to understand the context of some statements made in these documents. For instance, in one of Samsung's privacy policy documents, it was stipulated that they do collect even sensitive data through their smart TVs. It is important to try and understand the context of their statement.

This was achieved by looking at documents from different reviewers. For instance, one reviewer may take out of context a statement made by a manufacturer. By reviewing different documents, it was possible to make sure certain statements are not taken out of context.

III. The principle of interaction between the researcher and the subjects

Although no direct participants were used in this research, this principle does apply to this research in that the data collected from online reviews, is viewed as an interview with no questions used.

IV. The principle of abstraction and generalization

This principle is applied in chapter 5 where Content analysis method is used to analyzed data collected from manufacturers and reviewers. Using the discussion in chapter 5, users can follow as to how the researcher was able to reach his conclusion. The similarities indicated in this chapter in terms of security concerns and therefore guidelines for specific devices along with the generic guidelines from theory support the argument that smart devices has comparable risks.

V. *The principle of dialogical reasoning*

The objectives of this research were a priori theory that needed to prove through the findings from data. From the data collected and analyzed, there are certain security aspects of smart devices and appliances that could not be put solely on the devices, thus the researcher needs to reconcile some of theory that guided the research. For instance, it was found that the problem is not with the appliances or devices themselves, but rather the addition of smart features such as sensors, as well as negative security policy implications from the manufacturers in terms of data management.

VI. *The principle of multiple interpretations*

This principle was applied by reviewing multiple documents on the same devices. This helped in making sure that the researcher got the correct information by looking at a certain view from a multiple angle.

VII. *The principle of suspicion*

This principle was followed by making use of multiple reviewers. This helped in making sure that there are no biases in the interpretation of the data.

7.4.2 **Limitations of the study**

Currently there are tens of smart home appliances and devices on the market. It was not possible to investigate each smart device in each category. The solution was to group them into categories. The assumption is that each device in the four categories considered in this research, is represented of the whole. For instance, a smart fridge might have similarities with a smart washing machine or stove.

The second limitation of the research is that some model of the devices investigated are not very new. The reason for this choice is that, with older devices there more that is published as compared to new devices where sometimes no reviews could be found.

The third limitation was the difficulty with online documents. It was difficult sometime to find the correct documents to evaluate and some of the websites got updated during the course of the research, so some references we no longer available or contain different information.

7.5 FUTURE WORK

In this research, content analysis method, as used in social science (Chapter 2), was adopted. This manual method of analysing text document proved to be tedious. This resulted in the analysis process being slow, and the number or analysed documents few. All the documents that were analysed are easily found on the internet and some can easily be downloaded. Future work will be carried out to explore the possibility of using data mining techniques to mine for these documents, thus extending the number of documents that can be analysed. A method such as lexicon-based sentiment analysis can be used (Al-Ayyoub *et al.*, 2015:1) . This computerised text analysis approach makes use of artificial intelligence to train a system to be able classify text. The results of the manual and the AI approach can then be compared to see if the AI can improve the content analysis of smart devices' reviews.

7.6 SUMMARY

The purpose of this study was to identify security threats posed by smart home devices to unsuspecting homeowners in relation to their privacy in a home area network. Using the data collected from manufacturers' documents and reviewers, it was established that there exist a real threat data privacy of users in home area networks. These threats have been identified from features that most of these smart devices come with, such as internet connectivity, presence of microphones and cameras, lack of built-in security in some devices, poorly designed software that are full of vulnerabilities, the hardware limitations that prevent mechanisms such as encryption to be used with most IoT devices. From the manufacturers' viewpoints, they might not see the potential dangers these devices can put homeowners at. There is no doubt that there is great potential and benefit to the smart technology for homeowners, but trust need to be earned. At the moment, there is lack of a unified way or a

standard of implementing security into the design of these products, since each technology is proprietary to each manufacturer. The heterogeneity of IoT technologies and the lack of a common standard, has opened up loopholes where products are brought to the market without proper security implementations. The data collected from these devices is a major privacy concern for users, especially when they are not fully aware of how their data is going to be used once collected. At times all that users have is the trust that the manufacturer will safeguard their privacy. Of course, this is not enough, hence for users to protect themselves better, they need to be knowledgeable about the technology they are using.

Until these shortfalls are addressed, peoples' homes will continue to be filled with vulnerable smart appliances and devices that will continue to put their data at risks of security breaches. The guidelines provided in this chapter, section 7.3 can be followed in the meantime by users who want to take the risks of continuing to use these devices, but by following these guidelines, users can mitigate the risk of attacks in their home area networks.

BIBLIOGRAPHY

Aazam, M., Khan, I., Alsaffar, A.A. & Huh, E.-N. 2014. Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. (*In. Applied Sciences and Technology (IBCAST)*, 2014 11th International Bhurban Conference on organised by: IEEE. p. 414-419).

Abbasi, A.A. & Younis, M. 2007. A survey on clustering algorithms for wireless sensor networks. *Computer communications*, 30(14):2826-2841.

Aboud, S.J., AL-Fayoumi, M.A., Al-Fayoumi, M. & Jabbar, H.S. 2008. An efficient RSA public key encryption scheme. (*In. Information Technology: New Generations*, 2008. ITNG 2008. Fifth International Conference on organised by: IEEE. p. 127-130).

Ahmad, M.S. 2010. Wpa too! *DEF CON*, 18.

Al-Ayyoub, M., Essa, S.B. & Alsmadi, I. 2015. Lexicon-based sentiment analysis of Arabic tweets. *IJSNM*, 2(2):101-114.

Al-Sarawi, S., Anbar, M., Alieyan, K. & Alzubaidi, M. 2017. Internet of Things (IoT) communication protocols. (*In. 2017 8th International conference on information technology (ICIT)* organised by: IEEE. p. 685-690).

Alagupandi, P., Ramesh, R. & Gayathri, S. 2014. Smart irrigation system for outdoor environment using Tiny OS. (*In. Computation of Power, Energy, Information and Communication (ICCPEIC)*, 2014 International Conference on organised by. p. 104-108).

Ali, I., Sabir, S. & Ullah, Z. 2019. Internet of things security, device authentication and access control: a review. *arXiv preprint arXiv:1901.07309*.

Ali, W., Dustgeer, G., Awais, M. & Shah, M.A. 2017. IoT based smart home: Security challenges, security requirements and solutions. (In. 2017 23rd International Conference on Automation and Computing (ICAC) organised by. p. 1-6).

Amaratunga, D., Baldry, D., Sarshar, M. & Newton, R. 2002. Quantitative and qualitative research in the built environment: application of “mixed” research approach. *Work study*, 51(1):17-31.

Amazon. 2019a. Alexa-Enabled Echo Device FAQs. https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230#GUID-1CDA0A16-3D5A-47C1-9DD8-FDEDB10381A3_GUID-420F1812-F241-466A-A381-64D43D015778 Date of access: 23/11/2019 2019.

Amazon. 2019b. Alexa and Echo devices are designed to protect your privacy. <https://www.amazon.com/b/?node=19149155011> Date of access: 23/11/2019 2019.

Amazon. 2019c. Alexa, Echo Devices, and Your Privacy. https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=GVP69FUJ48X9DK8V Date of access: 18/7/2019 2019.

Amazon. 2019d. Echo show. <https://www.amazon.com/All-new-Echo-Show-2nd-Gen/dp/B077SXWSRP#tech> Date of access: 19/11/2019 2019.

Amjad, M., Sharif, M., Afzal, M.K. & Kim, S.W. 2016a. TinyOS-New Trends, Comparative Views and Supported Sensing Applications: A Review. *Sensors Journal, IEEE*, PP(99):1-1.

TinyOS-New Trends, Comparative Views and Supported Sensing Applications: A Review, 1-1 2016b.

Anjum, F. & Mouchtaris, P. 2007. Security for wireless ad hoc networks: John Wiley & Sons.

Anon. 2011. IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads. *IEEE Std 2030-2011*:1-126.

Ansari, S., Rajeev, S. & Chandrashekar, H. 2002. Packet sniffing: a brief introduction. *Potentials, IEEE*, 21(5):17-19.

Antoniuk, L., Gernego, I., Dyba, V., Polishchuk, Y. & Sybirianska, Y. 2017. Barriers and opportunities for hi-tech innovative small and medium enterprises development in the 4th industrial revolution era. *Problems and Perspectives in Management*, 15(4):100-113.

Apple. 2019. Apple homepod. <https://www.apple.com/homepod/> Date of access: 8/8/2019 2019.

Arbaugh, W.A., Shankar, N., Wan, Y.J. & Zhang, K. 2002. Your 80211 wireless network has no clothes. *Wireless Communications, IEEE*, 9(6):44-51.

Arlo.com. 2019. Arlo pro 2. <https://www.arlo.com/en-us/landing/arlo-pro-2/> Date of access: 1/10/2019 2019.

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

August. 2019a. August policies and agreements <https://august.com/pages/privacy-policy> Date of access: 15/10/2019 2019.

August. 2019b. Smart Lock Pro + Connect. <https://august.com/products/august-smart-lock-pro-connect> Date of access: 1/10/2019 2019.

Baccelli, E., Hahm, O., Günes, M., Wählich, M. & Schmidt, T.C. Operating Systems for the IoT—Goals, Challenges, and Solutions.

Baccelli, E., Hahm, O., Günes, M., Wählisch, M. & Schmidt, T.C. 2013. RIOT OS: Towards an OS for the Internet of Things. (In. Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on organised by: IEEE. p. 79-80).

Baccelli, E., Hahm, O., Wählisch, M., Günes, M. & Schmidt, T. 2012. RIOT: One OS to Rule Them All in the IoT.

Baron, J. 2019. Google's New Nest Hub Max Raises Questions About How Much We Still Value Our Privacy <https://www.forbes.com/sites/jessicabaron/2019/09/09/googles-new-nest-hub-max-raises-questions-about-how-much-we-still-value-our-privacy/#5b86058b146b> Date of access: 24/11/2019 2019.

Bhartiya, S. 2017. Your smart fridge may kill you: The dark side of IoT. <https://www.infoworld.com/article/3176673/your-smart-fridge-may-kill-you-the-dark-side-of-iot.html> Date of access: 4/11/2019 2019.

Bhaskar, S. 2008. Information Security: A Practical Approach: Alpha Science International, Ltd.

Bishop, M. 2005. Introduction to computer security: Addison-Wesley Boston, MA.

Bitzer, B. & Gebretsadik, E.S. 2013. Cloud computing framework for smart grid applications. (In. Power Engineering Conference (UPEC), 2013 48th International Universities' organised by. p. 1-5).

Blanco, M.A. & Marco, R. 2003. Network access authentication system: Google Patents.

Blecher, J. 2018. Samsung Family Hub Refrigerator review. <https://www.digitaltrends.com/appliance-reviews/samsung-family-hub-refrigerator-review/> Date of access: 04/11/2019 2018.

Blessing, L.T. & Chakrabarti, A. 2009. DRM, a design research methodology: Springer Science & Business Media.

Boell, K.S.C.-K., Dubravka. 2010. Literature Reviews and the Hermeneutic Circle. *Australian Academic & Research Libraries*, 41(2):129-144.

Bohman, J. 2005. Critical theory.

Bowen, G.A. 2009. Document analysis as a qualitative research method. *Qualitative research journal*, 9(2):27-40.

Brandom, R. 2017. Here's how to use the CIA's 'weeping angel' smart TV hack. <https://www.theverge.com/2017/4/25/15421326/smart-tv-hacking-cia-samsung-weeping-angel-vulnerability> Date of access: 27/05/2019 2019.

Brickell, E.F. 1989. A survey of hardware implementations of RSA. (In. Conference on the Theory and Application of Cryptology organised by: Springer. p. 368-370).

Britt, J., Matsumura, S., Forood, H., Zimmerman, S., Myles, P., Zawicki, S., et al. 2017. System and method for notifying a user of conditions associated with an internet-of-things (IoT) hub: Google Patents.

Bruni, P., Garcia, R., Kaschta, S., Klitsch, J., Kumar, R., Lurie, A., et al. 2014. DB2 10 for z/OS Technical Overview: IBM Redbooks.

Bryman, A. 2006. Paradigm peace and the implications for quality. *International Journal of Social Research Methodology*, 9(2):111-126.

BuisnessWire. 2018. 200 Million Homes Now Have an Ultra HD TV, Says Strategy Analytics. <https://www.businesswire.com/news/home/20181206005556/en/200-Million-Homes-Ultra-HD-TV-Strategy> Date of access: 02/04/2019 2019.

businessKorea. 2019. Samsung's Global TV Market Share Projected to Have Fall below 20% in 2018. <http://www.businesskorea.co.kr/news/articleView.html?idxno=28490> Date of access: 02/04/2019 2019.

Buttyán, L. & Dóra, L. 2006. WiFi Security–WEP and 802.11 i. *EURASIP Jthisnal on Wireless Communication and Networking*(1):1-13.

canary.is. 2019. Canary Flex. <https://canary.is/flex/> Date of access: 1/10/2019 2019.

Canonical. 2017. Taking charge of the IoT's security vulnerabilities. <https://pages.ubuntu.com/IoT-Security-whitepaper.html> Date of access: 24/10/2019 2019.

Carroll, J.M. 2014. Computer security: Butterworth-Heinemann.

Carter, B. & Magoc, T. 2007. Classical Ciphers and Cryptanalysis. *space*, 1000:1.

Chandane, M., Bhirud, S. & Bonde, S. 2012. Performance analysis of IEEE 802.15. 4. *International Journal of Computer Applications*, 40(5):23-29.

Chandra, S., Paira, S., Alam, S.S. & Sanyal, G. 2014. A comparative survey of Symmetric and Asymmetric Key Cryptography. (In. Electronics, Communication and Computational Engineering (ICECCE), 2014 International Conference on organised by. p. 83-93).

Chen, D. & Zhao, H. 2012. Data security and privacy protection issues in cloud computing. (In. Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on organised by: IEEE. p. 647-651).

Chin, M. 2019. Amazon Echo Show (2nd Gen) Review: Better In Every Way. <https://www.tomsguide.com/us/amazon-echo-show-2nd-gen,review-5758.html> Date of access: 24/11/2019 2019.

Cisco. 2019. Internet of Things. <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf?dtid=osscdc000283> Date of access: 14/10/2019 2019.

Clark, D.D., Pogran, K.T. & Reed, D.P. 1978. An introduction to local area networks. *Proceedings of the IEEE*, 66(11):1497-1517.

Contiki-os.org. 2016. Other Contiki platforms. <http://www.contiki-os.org/hardware.html> Date of access: 14/01/2016 2016.

Coopridier, N., Archer, W., Eide, E., Gay, D. & Regehr, J. 2007. Efficient memory safety for TinyOS. (In. Proceedings of the 5th international conference on Embedded networked sensor systems organised by: ACM. p. 205-218).

Corbin, J. & Morse, J.M. 2003. The Unstructured Interactive Interview: Issues of Reciprocity and Risks when Dealing with Sensitive Topics. *Qualitative Inquiry*, 9(3):335-354.

Corbin, J.M. & Strauss, A. 1990. Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative sociology*, 13(1):3-21.

Crist, R. 2019a. Amazon and Google are listening to your voice recordings. Here's what we know about that. <https://www.cnet.com/how-to/amazon-and-google-are-listening-to-your-voice-recordings-heres-what-we-know/> Date of access: 24/11/2019 2019.

Crist, R. 2019b. Google's got a new face-tracking camera for your home. We've got questions. <https://www.cnet.com/news/google-nest-hub-max-a-new-face-tracking-camera-for-your-home-weve-got-questions/> Date of access: 24/11/2019 2019.

Crist, R. 2019c. Google Nest Hub Max review. <https://www.cnet.com/reviews/google-nest-hub-max-the-bigger-nest-hub-isnt-the-better-one-review/> Date of access: 24/11/2019 2019.

Cyware.com. 2019. Android-based Sony Smart TVs expose Wi-fi passwords and stored images due to security bugs <https://cyware.com/news/android-based-sony-smart-tvs-expose-wi-fi-passwords-and-stored-images-due-to-security-bugs-bf5c0cec> Date of access: 23/08/2019 2019.

Dai, H.-N., Wang, Q., Li, D. & Wong, R.C.-W. 2013. On eavesdropping attacks in wireless sensor networks with directional antennas. *International Journal of Distributed Sensor Networks*, 2013.

Darke, P., Shanks, G. & Broadbent, M. 1998. Successfully completing case study research: combining rigour, relevance and pragmatism. *Information Systems Journal*, 8(4):273-289.

Datta, S.K., Bonnet, C. & Nikaein, N. 2014. An iot gateway centric architecture to provide novel m2m services. (In. Internet of Things (WF-IoT), 2014 IEEE World Forum on organised by: IEEE. p. 514-519).

Dede, A., Della Giustina, D., Rinaldi, S., Ferrari, P., Flammini, A. & Vezzoli, A. 2015. Smart meters as part of a sensor network for monitoring the low voltage grid. (In. Sensors Applications Symposium (SAS), 2015 IEEE organised by: IEEE. p. 1-6).

Delaney, J.R. 2019. The Best Smart Locks for 2019. <https://www.pcmag.com/article/344336/the-best-smart-locks> Date of access: 1/10/2019 2019.

Depuru, S.S.S.R., Wang, L. & Devabhaktuni, V. 2011. Smart meters for power grid: Challenges, issues, advantages and status. *Renewable and sustainable energy reviews*, 15(6):2736-2742.

Dhar, S.K., Bhunia, S.S. & Mukherjee, N. 2014. Interference Aware Scheduling of Sensors in IoT Enabled Health-Care Monitoring System. (In. Emerging Applications of Information

Technology (EAIT), 2014 Fourth International Conference of organised by: IEEE. p. 152-157).

Dictionary.com. 2019. <http://www.dictionary.com/browse/crypto> Date of access: 25/10/2019.

Dieronitou, I. 2014. The ontological and epistemological foundations of qualitative and quantitative approaches to research. *International Journal of Economics*, 2(10):1-17.

Dirienzo, T.P., Krishnan, N.A., Srija & Santos, J.R. 2014. Effects of smart appliances on residential consumption patterns. (In. Systems and Information Engineering Design Symposium (SIEDS), 2014 organised by. p. 188-192).

Douglas, N. 2017. We Asked Five Security Experts If Smart Locks Are Ever Safe. <https://lifehacker.com/we-asked-five-security-experts-if-smart-locks-are-ever-1797910643>
Date of access: 29/10/2019 2019.

Driscoll, D.L., Appiah-Yeboah, A., Salib, P. & Rupert, D.J. 2007. Merging qualitative and quantitative data in mixed methods research: How to and why not.

Dube, D. & Ramanarayanan, S. 2004. Internet banking—a layered approach to security. (In. International Conference on Intelligent Information Technology organised by: Springer. p. 190-197).

Dunkels, A., Grönvall, B. & Voigt, T. 2004. Contiki-a lightweight and flexible operating system for tiny networked sensors. (In. Local Computer Networks, 2004. 29th Annual IEEE International Conference on organised by: IEEE. p. 455-462).

Easttom II, W.C. 2019. Computer security fundamentals: Pearson IT Certification.

ElectronicsTutorials. 2015. Sensors and Transducers. http://www.electronicstutorials.ws/io/io_1.html Date of access: 10/11/2015.

Elkaduwe, D., Derrin, P. & Elphinstone, K. 2008. Kernel design for isolation and assurance of physical memory. (In. Proceedings of the 1st workshop on Isolation and integration in embedded systems organised by: ACM. p. 35-40).

Elliot, J. 2019. A Guide to Smart Refrigerators. <https://www.mansionglobal.com/articles/a-guide-to-smart-refrigerators-201776> Date of access: 4/11/2019 2019.

Elo, S. & Kyngäs, H. 2008. The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1):107-115.

Emara, K., Abdeen, M. & Hashem, M. 2009. A gateway-based framework for transparent interconnection between WSN and IP network. (In. EUROCON 2009, EUROCON'09. IEEE organised by: IEEE. p. 1775-1780).

Erol-Kantarci, M. & Mouftah, H.T. 2015. Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues. *Communications Surveys & Tutorials, IEEE*, 17(1):179-197.

Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F.B., Rodriguez, J., Bicaku, A., et al. 2019. A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment. *IEEE Internet of Things Journal*, 6(1):288-296.

ETF. 2017. RFC. <https://www.ietf.org/rfc.html> Date of access: 23/03/2017.

Farag, M.M., Azab, M. & Mokhtar, B. 2014. Cross-layer security framework for smart grid: Physical security layer. (In. Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2014 IEEE PES organised by. p. 1-7).

Farooq, M.O. & Kunz, T. 2011. Operating systems for wireless sensor networks: A survey. *Sensors*, 11(6):5900-5930.

Ferguson, N. & Schneier, B. 2000. A cryptographic evaluation of IPsec. *Counterpane Internet Security, Inc*, 3031.

Fertik, M. 2012. Your future boss is watching you online. You should be too. <https://hbr.org/2012/04/your-future-employer-is-watchi> Date of access: 05/03/2019 2019.

Fisch, E.A., White, G.B. & Pooch, U.W. 2017. Computer system and network security: CRC press.

Fournaris, A.P. & Koufopavlou, O. 2005. A new RSA encryption architecture and hardware implementation based on optimized Montgomery multiplication. (In. 2005 IEEE International Symposium on Circuits and Systems organised by: IEEE. p. 4645-4648).

Francillon, A. & Castelluccia, C. 2008. Code injection attacks on harvard-architecture devices. (In. Proceedings of the 15th ACM conference on Computer and communications security organised by: ACM. p. 15-26).

Frangos, J.-M. 2017. The Internet of Things will power the Fourth Industrial Revolution. <https://www.weforum.org/agenda/2017/06/internet-of-things-will-power-the-fourth-industrial-revolution/> Date of access: 2019.

Frost Gorder, P. 2003. Sizing up smart dust. *Computing in Science & Engineering*, 5(6):6-9.

Frustaci, M., Pace, P., Aloï, G. & Fortino, G. 2018. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal*, 5(4):2483-2495.

Gaillet, L., xe & e, L. 2012. (Per)Forming Archival Research Methodologies. *College Composition and Communication*, 64(1):35-58.

Gao, J., Xiao, Y., Liu, J., Liang, W. & Chen, C.P. 2012. A survey of communication/networking in Smart Grids. *Future Generation Computer Systems*, 28(2):391-404.

Gartner. 2014. Gartner Says IoT Security Requirements Will Reshape and Expand Over Half of Global Enterprise IT Security Programs by 2020. <http://www.gartner.com/newsroom/id/2727017> Date of access: 3/3/2016 2016.

Gartner. 2019. Internet Of Things. <https://www.gartner.com/en/information-technology/glossary/internet-of-things> Date of access: 14/10/2019 2019.

Garzia, F. 2013. Handbook of communications security: WIT Press.

GE. 2019a. CONNECTED DATA PRIVACY POLICY GE WiFi Connect Appliances. https://www.geappliances.com/privacy/privacy_policy_connected.htm Date of access: 8/10/2019 2019.

GE. 2019b. GE Connect. https://www.geappliances.com/ge/connected-appliances/?icid=GEA_Connect Date of access: 8/10/2019 2019.

GE. 2019c. GE Profile Series smart fridge user manual. <https://products.geappliances.com/MarketingObjectRetrieval/Dispatcher?RequestType=PDF&Name=49-60792-3.pdf> Date of access: 28/8/2019 2019.

Geerts, G.L. 2011. A design science research methodology and its application to accounting information systems research. *International Journal of Accounting Information Systems*, 12(2):142-151.

Gerring, J. 2006. Case study research: Principles and practices: Cambridge University Press.

Gibbs, S. 2019. Google Nest Hub Max review: bigger, better and smarter display. <https://www.theguardian.com/technology/2019/nov/06/google-nest-hub-max-review-display-camera-facial-recognition> Date of access: 24/11/2019 2019.

Glaser, B. 2017. Discovery of grounded theory: Strategies for qualitative research: Routledge.

Google. 2019a. Data security & privacy on Google Home. <https://support.google.com/googlenest/answer/7072285?hl=en> Date of access.

Google. 2019b. Explore what you can do with Google Home. <https://support.google.com/googlehome/answer/7130274?hl=en> Date of access: 02/04/2019 2019.

Google. 2019c. FAQs on privacy: Google Nest. https://support.google.com/googlenest/answer/9415830?hl=en&ref_topic=7173611 Date of access: 23/11/2019 2019.

Google. 2019d. Google nest hub max. https://store.google.com/gb/product/google_nest_hub_max_tech_specs?hl=en-GB Date of access: 19/11/2019 2019.

Green, T. 2015. Gartner: Makers of things for Internet of Things undervalue security. <http://www.networkworld.com/article/2883637/security0/gartner-makers-of-things-for-internet-of-things-undervalue-security> Date of access: 24/03/2015 2015.

Greenwood, D.J. & Levin, M. 2006. Introduction to action research: Social research for social change: SAGE publications.

Gregor, S. 2006. The nature of theory in information systems. *MIS quarterly*:611-642.

Gregor, S. & Hevner, A.R. 2013. Positioning and presenting design science research for maximum impact. *Mis Quarterly*, 37(2):337-355.

Grogan, A. 2012. Smart appliances. *Engineering & Technology*, 7(6):44-45.

Haller, S. 2010. The things in the internet of things. *Poster at the (IoT 2010). Tokyo, Japan, November*, 5:26.

Hamalainen, P., Alho, T., Hannikainen, M. & Hamalainen, T.D. 2006. Design and implementation of low-area and low-power AES encryption hardware core. (In. 9th EUROMICRO Conference on Digital System Design (DSD'06) organised by: IEEE. p. 577-583).

Harrison, O. & Waldron, J. 2007. AES encryption implementation and analysis on commodity graphics processing units. (In. International Workshop on Cryptographic Hardware and Embedded Systems organised by: Springer. p. 209-226).

Heath, H. & Cowley, S. 2004. Developing a grounded theory approach: a comparison of Glaser and Strauss. *International journal of nursing studies*, 41(2):141-150.

Heinzman, A. 2019. Your Expensive Smart Appliance May Not Last A Decade. <https://www.howtogeek.com/401635/your-expensive-smart-appliance-may-not-last-a-decade/> Date of access: 03/11/2019 2019.

Hernandez, G., Arias, O., Buentello, D. & Jin, Y. 2014. Smart nest thermostat: A smart spy in your home. *Black Hat USA*.

Hevner, A. & Chatterjee, S. 2010. Design science research in information systems: Springer.

Hoque, N., Bhuyan, M.H., Baishya, R.C., Bhattacharyya, D.K. & Kalita, J.K. 2014. Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40:307-324.

HP. 2014. HP Study Finds Nearly 70 Percent of IT Professionals Experience Weekly Phishing Attacks. <http://www8.hp.com/us/en/hp-news/press-release.html?id=1763561#.V0xFqulmQ5o> Date of access: 30/5/2016 2016.

Hsieh, H.-F. & Shannon, S.E. 2005. Three approaches to qualitative content analysis. *Qualitative health research*, 15(9):1277-1288.

Hu, F., Celentano, L. & Xiao, Y. 2009. Error-resistant RFID-assisted wireless sensor networks for cardiac telehealthcare. *Wireless Communications and Mobile Computing*, 9(1):85-101.

Hussain, S., Schaffner, S. & Moseychuck, D. 2009. Applications of wireless sensor networks and RFID in a smart home environment. (In. Communication Networks and Services Research Conference, 2009. CNSR'09. Seventh Annual organised by: IEEE. p. 153-157).

Hyde, K.F. 2000. Recognising deductive processes in qualitative research. *Qualitative market research: An international journal*, 3(2):82-90.

Hyde, P. 2019. The 7 Best Smart Fridges of 2019. <https://www.lifewire.com/best-smart-fridges-4159454> Date of access: 28/8/2019 2019.

Hyeyeon, K., Kyung-Yul, C. & Aesoon, P. 2007. Analysis of WLAN to UMTS Handover. (In. Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th organised by. p. 184-188).

Hyland, K. 2016. Methods and methodologies in second language writing research. *System*, 59:116-125.

IBT. 2012. Smart Energy Meters in UK Homes Pose Energy Threat. <http://www.ibtimes.co.uk/energy-meter-foreign-terror-gchq-security-british-350490> Date of access: 3/3/2016 2016.

IEEE. 2006. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). NY, USA: IEEE.

ITweb. 2017. LG's SmartThinQ vulnerability exposes millions. <https://www.itweb.co.za/content/rKPNG8v8g1jq4mwD> Date of access: 4/11/2019 2019.

Javed, F., Afzal, M.K., Sharif, M. & Kim, B.-S. 2018. Internet of Things (IoT) operating systems support, networking technologies, applications, and challenges: A comparative review. *IEEE Communications Surveys & Tutorials*, 20(3):2062-2100.

Jawandhiya, P.M., Ghonge, M.M., Ali, M. & Deshpande, J. 2010. A survey of mobile ad hoc network attacks. *International Journal of Engineering Science and Technology*, 2(9):4063-4071.

Jia, X., Feng, Q., Fan, T. & Lei, Q. 2012. RFID technology and its applications in Internet of Things (IoT). (In. Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on organised by: IEEE. p. 1282-1285).

Johnson, R.B. & Onwuegbuzie, A.J. 2004. Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, 33(7):14-26.

Jonsson, J. & Kaliski Jr, B.S. 2002. On the Security of RSA Encryption in TLS. (In. Annual International Cryptology Conference organised by: Springer. p. 127-142).

Jun-Hyuk, C., Yeon-Kyung, W., Seung-Man, C. & Jong-Tae, P. 2013. A secure WLAN access sharing system using SNS. (In. Communications Workshops (ICC), 2013 IEEE International Conference on organised by. p. 761-765).

Kaliski, B. 1998. PKCS# 1: RSA encryption version 1.5. <https://tools.ietf.org/html/rfc2313> Date of access: 29/11/2019 2019.

Kandukuri, B.R., Paturi, V.R. & Rakshit, A. 2009. Cloud security issues. (In. Services Computing, 2009. SCC'09. IEEE International Conference on organised by: IEEE. p. 517-520).

Karnain, M.A.B. & Zakaria, Z.B. 2015. A Review on ZigBee Security Enhancement in Smart Home Environment. (In. 2015 2nd International Conference on Information Science and Security (ICISS) organised by. p. 1-4).

Kats, R. 2018. How Many Households Own a Smart TV? <https://www.emarketer.com/content/how-many-households-own-a-smart-tv> Date of access: 8/11/2019 2019.

Kavitha, T. & Sridharan, D. 2010. Security vulnerabilities in wireless sensor networks: A survey. *Journal of information Assurance and Security*, 5(1):31-44.

Kendall, J. 1999. Axial coding and the grounded theory controversy. *Western journal of nursing research*, 21(6):743-757.

Kester, Q.-A. 2013. A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher. *arXiv preprint arXiv:1307.7786*.

Khan, M.A. & Salah, K. 2018. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395-411.

Khan, T., Khan, A., Babar, M., Taj, T. & Ijaz, I. 2014. Smart meter incorporating UWB technology. (In. Electrical and Electronic Engineering Conference (ElConRusNW), Proceedings of the 2014 IEEE NW Russia Young Researchers in organised by: IEEE. p. 75-78).

Kinsella, B. 2019. Alibaba Dominates China Smart Speaker Sales with 41.2% Share. <https://voicebot.ai/2019/02/21/alibaba-dominates-china-smart-speaker-sales-with-41-2-share/> Date of access: 05/06/2019.

Klein, H.K. & Myers, M.D. 1999. A set of principles for conducting and evaluating interpretive field studies in information systems. *Mis Quarterly*:67-93.

Koch, R. 2019. The privacy risks of smart speakers like Amazon Echo, Apple HomePod, and Google Home. <https://securityboulevard.com/2019/01/the-privacy-risks-of-smart-speakers-like-amazon-echo-apple-homepod-and-google-home/> Date of access: 18/7/2019 2019.

Lamaazi, H., Benamar, N., Jara, A.J. & Ladid, L. 2014. Challenges of the Internet of Things: IPv6 and Network Management. (In. Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2014 Eighth International Conference on organised by: IEEE. p. 328-333).

Lau, J., Zimmerman, B. & Schaub, F. 2018. Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):102.

Leary, B. 2019. As Smart Speakers Rise in Popularity, Synthetic Speech and Voice Synthesis is Something We Need to be Ready For. <https://smallbiztrends.com/2019/01/voice-assistant-security-concerns.html> Date of access: 05/06/2019 2019.

Leavitt, N. 2011. Mobile security: finally a serious problem? *Computer*, 44(6):11-14.

Lenovo. 2019. What are smart speakers and smart displays? <https://www.lenovo.com/za/en/faqs/voice-search-faqs/what-is-smart-speaker-display/> Date of access: 1/10/2019 2019.

Leonardo, Z. 2004. Critical social theory and transformative knowledge: The functions of criticism in quality education. *Educational Researcher*, 33(6):11-18.

Levis, P., Madden, S., Polastre, J., Szewczyk, R., Whitehouse, K., Woo, A., et al. 2005. Tinyos: An operating system for sensor networks. *Ambient intelligence*. Springer. p. 115-148).

LG. 2012. WT6001HV.

LG. 2019a. Legal Documents (Smart TV). http://gb.lgappstv.com/appspc/footer/footer/moveDeviceTerms.lge?type=S_PRG&level=2&link=202 Date of access: 02/04/2019 2019.

LG. 2019b. LG 65SM8600PUA LED TV USER MANUAL. <http://gscs-b2c.lge.com/downloadFile?fileId=dDn3wn5I2hh2HHQA18gBQQ> Date of access.

LG. 2019c. OWNER'S MANUAL FOR LG MFL69668847 INSTAVIEW SMART FRIDGE: LG.

LG. 2019d. Smarththing. <https://www.lg.com/us/discover/smarththing/thing> Date of access.

Li, H., Jia, Z. & Xue, X. 2010. Application and Analysis of ZigBee Security Services Specification. (In. 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing organised by. p. 494-497).

Liberium. 2016. Security in 802.15.4 and ZigBee networks. <http://www.libelium.com/security-802-15-4-zigbee/> Date of access: 30/6/2016.

Life, R.S. 1994. Qualitative data analysis.

Lloyd, C. 2018. Are Your Smarthome Devices Spying on You? <https://www.howtogeek.com/366990/are-your-smarthome-devices-spying-on-you/> Date of access: 04/11/2019 2019.

Logitech. 2019. Circle 2 home security camera. <https://www.logitech.com/en-us/product/circle-2-home-security-camera> Date of access: 29/11/2019 2019.

Lu, C.-C. & Tseng, S.-Y. 2002. Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. (In. Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on organised by: IEEE. p. 277-285).

Lu, C.-W., Li, S.-C. & Wu, Q. 2011. Interconnecting ZigBee and 6LoWPAN wireless sensor networks for smart grid applications. (In. Sensing Technology (ICST), 2011 Fifth International Conference on organised by: IEEE. p. 267-272).

Lu, J., Sookoor, T., Srinivasan, V., Gao, G., Holben, B., Stankovic, J., et al. 2010. The smart thermostat: using occupancy sensors to save energy in homes. (In. Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems organised by: ACM. p. 211-224).

Luciano, D. & Prichett, G. 1987. Cryptology: From Caesar ciphers to public-key cryptosystems. *The College Mathematics Journal*, 18(1):2-17.

Ludlow, D. 2019. Samsung SmartThings V3 Review <https://www.trustedreviews.com/reviews/samsung-smarthings-v3> Date of access: 25/11/2019 2019.

Mao, W. 2003. Modern cryptography: theory and practice: Prentice Hall Professional Technical Reference.

Market.us. 2019. Smartphone Brands Statistics and Facts 2019. <https://market.us/statistics/smartphone-brands/> Date of access: 26/11/2019 2019.

Mason, A. 2015. SENSORS a.k.a. Interfacing to the Real World: Review of Electrical Sensors and Actuators. <http://www.egr.msu.edu/classes/ece480/capstone/480-sensors.pdf> Date accessed: 10/11/2015.

Matyszczuk, C. 2015. Samsung changes Smart TV privacy policy in wake of spying fears. <https://www.cnet.com/news/samsung-changes-smarttv-privacy-policy-in-wake-of-spying-fears/> Date of access: 03/05/2019 2019.

McGraw, G. 2004. Software security. *IEEE Security & Privacy*, 2(2):80-83.

McLaughlin, J.E., Bush, A.A. & Zeeman, J.M. 2016. Mixed methods: Expanding research methodologies in pharmacy education. *Currents in Pharmacy Teaching and Learning*, 8(5):715-721.

Meyers, M. 2015. Qualitative Research in Information Systems. <http://www.qual.auckland.ac.nz>. Date of access: 05/03/2019 2019.

Michele, B. & Karpow, A. 2014. Watch and be watched: Compromising all Smart TV generations. (In. Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th organised by. p. 351-356).

Micro, T. 2014. Smart Lock Devices: Security Risks and Opportunities <https://blog.trendmicro.com/trendlabs-security-intelligence/smart-lock-devices-security-risks-and-opportunities/> Date of access: 28/10/2019 2019.

Midrack, R.L. 2019. What is a Smart Lock and Why Would You Want One? <https://www.lifewire.com/smart-locks-4159894> Date of access: 1/10/2019 2019.

Miller, M. 2015. The internet of things: How smart TVs, smart cars, smart homes, and smart cities are changing the world: Pearson Education.

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

Mishra, A. & Arbaugh, W.A. 2002. An initial security analysis of the IEEE 802.1 X standard.

MIT. 2016. Protecting Data. https://ist.mit.edu/security/protecting_data Date of access: 7/6/2016.

Mois, G., Folea, S. & Sanislav, T. 2017. Analysis of three IoT-based wireless sensors for environmental monitoring. *IEEE Transactions on Instrumentation and Measurement*, 66(8):2056-2064.

Mousa, A. & Hamad, A. 2006. Evaluation of the RC4 Algorithm for Data Encryption. *IJCSA*, 3(2):44-56.

Moyle, W. 2002. Unstructured interviews: challenges when participants have a major depressive illness. *Journal of Advanced Nursing*, 39(3):266-273.

Musaddiq, A., Zikria, Y.B., Hahm, O., Yu, H., Bashir, A.K. & Kim, S.W. 2018. A survey on resource management in IoT operating systems. *IEEE Access*, 6:8459-8482.

Myers, M.D. 1997. Qualitative research in information systems. *Management Information Systems Quarterly*, 21(2):241-242.

Namboodiri, V., Aravinthan, V., Mohapatra, S.N., Karimi, B. & Jewell, W. 2014. Toward a secure wireless-based home area network for metering in smart grids. *Systems Journal, IEEE*, 8(2):509-520.

Narmada, A. & Rao, P.S. 2012. Zigbee Based WSN with IP Connectivity.178-181.

Ngwenyama, O.K. 1991. The critical social theory approach to information systems: problems and challenges. *Information systems research: Contemporary approaches and emergent traditions*:267-280.

Ni, J., Zhang, K., Lin, X. & Shen, X.S. 2018. Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. *IEEE Communications Surveys & Tutorials*, 20(1):601-628.

Nohe, P. 2017. Hacking IoT Devices: How to Create a Botnet of Refrigerators. <https://www.thesslstore.com/blog/hacking-iot-devices-create-botnet-refrigerators/> Date of access: 4/11/2019 2019.

Null, C. 2018. Samsung SmartThings Hub (2018) review: Samsung's smart hub finally goes wireless. <https://www.techhive.com/article/3384916/samsung-smarthings-hub-2018-review-samsung-s-smart-hub-finally-goes-wireless.html> Date of access: 25/11/2019 2019.

Owen, M. 2019. HomePod sales up in fourth quarter, Amazon and Google extending lead. <https://appleinsider.com/articles/19/02/19/homepod-sales-up-in-fourth-quarter-amazon-and-google-extending-lead> Date of access: 05/06/2019.

Panajotovic, B., Jankovic, M. & Odadzic, B. 2011. ICT and smart grid. (In. Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), 2011 10th International Conference on organised by. p. 118-121).

Panda. 2018. Which is the safest smart speaker?
<https://www.pandasecurity.com/mediacenter/technology/which-is-the-safest-smart-speaker/>

Date of access: 04/06/2019 2019.

Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L. & Chen, H. 2014. Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT). (In. 2014 IEEE Joint Intelligence and Security Informatics Conference organised by. p. 232-235).

Paul, J. 2017. Samsung's Linux Based Tizen OS Is A Security Nightmare.
<https://itsfoss.com/tizen-os-security/> Date of access: 03/11/2019 2019.

Paul, T. & Kumar, G.S. 2009. Safe Contiki OS: Type and Memory Safety for Contiki OS. (In. Advances in Recent Technologies in Communication and Computing, 2009. ARTCom '09. International Conference on organised by. p. 169-171).

Peev, G. 2012. Government plans to install smart meters in our homes will leave us open to cyber attack. <http://www.dailymail.co.uk/news/article-2156648/Government-plans-install-smart-meters-homes-leave-open-cyber-attack.html> Date accessed: 24/03/2015.

Perez, J. & Mahdy, A. 2008. A Survey of Wireless Network Security Protocols. *Journal of Computing Sciences in Colleges, Electronic Issue*.

Pfleeger, C.P. & Pfleeger, S.L. 2012. Analyzing computer security: a threat/vulnerability/countermeasure approach: Prentice Hall Professional.

Pi Huang, A. 2016. <http://electronicdesign.com/communications/understanding-ieee-80211ac-vht-wireless> Date accessed: 03/02/2016.

Polianytzia, A., Starkova, O. & Herasymenko, K. 2016. Survey of hardware IoT platforms. (In. 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T) organised by: IEEE. p. 152-153).

Pope, C., Ziebland, S. & Mays, N. 2000. Qualitative research in health care: analysing qualitative data. *BMJ: British Medical Journal*, 320(7227):114.

Postscapes.com. 2019. IoT Standards and Protocols. <https://www.postscapes.com/internet-of-things-protocols/> Date of access: 28/02/2019 2019.

Price, M. 2018. Are you setting your smart lock up for intrusion? <https://www.cnet.com/news/how-you-might-be-setting-your-smart-lock-up-for-intrusion/> Date of access: 29/10/2019 2019.

prnewswire.com. 2019. LG Brings Slow-Melting Round 'Craft Ice' To Flagship InstaView Refrigerators. <https://www.prnewswire.com/news-releases/lg-brings-slow-melting-round-craft-ice-to-flagship-instaview-refrigerators-300908181.html> Date of access: 4/11/2019 2019.

Prospero, M. 2019a. Best Smart Home Hubs of 2019. <https://www.tomsguide.com/us/best-smart-home-hubs,review-3200.html> Date of access: 19/11/2019 2019.

Prospero, M. 2019b. Samsung SmartThings Hub V3 Review: Still the Best, But Could Be Better. <https://www.tomsguide.com/us/samsung-smart-things-v3,review-5809.html> Date of access: 25/11/2019 2019.

protectamerica.com. 2018. Are Smart Door Locks Safe?: Three Things to Keep in Mind. https://www.protectamerica.com/home-security-blog/safe-sound/are-smart-door-locks-safe-three-things-to-keep-in-mind_20027 Date of access: 29/10/2019 2019.

Purdy, J. 2011. Three gifts of digital archives. *Journal of Literacy and Technology*, 12(3):24-49.

Ramya, C.M., Shanmugaraj, M. & Prabakaran, R. 2011. Study on ZigBee technology. (In. 2011 3rd International Conference on Electronics Computer Technology organised by: IEEE. p. 297-301).

Raphael, T.J. 2015. Your smart TV may be spying on you — and stopping it is against the law. <https://www.pri.org/stories/2015-02-13/your-smart-tv-may-be-spying-you-and-stopping-it-against-law> Date of access: 06/05/2019 2019.

Rapley, T. & Jenkins, K.N. 2010. Document Analysis A2 - Peterson, Penelope. (In Baker, E. & McGraw B., eds. International Encyclopedia of Education (Third Edition). Oxford: Elsevier. p. 380-385).

Rasuba, M., Khuluse, S. & Elphinstone, C. 2010. Forecasts for electricity demand in South Africa (2010–2035) using the CSIR sectoral regression model.

Rawat, D.B. & Bajracharya, C. 2015. Cyber security for smart grid systems: Status, challenges and perspectives. (In. SoutheastCon 2015 organised by. p. 1-6).

Rawnsley, M.M. 1998. Ontology, Epistemology, and Methodology: A Clarification. *Nursing Science Quarterly*, 11(1):2-4.

Reid, A., Lorenz, J. 2008. Network for Home and Small Businesses. 3. Indianapolis, IN: Cisco Press.

Reuters. 2018. Global Smart TV Market 2018-2025 Trends, Growth, Brands, Features and Key Players Analysis (Samsung Electronics, LG Electronics, Sony, Xiaomi, Philips...). <https://www.reuters.com/brandfeatures/venture-capital/article?id=49143> Date of access: 02/04/2019 2019.

RIOT. 2015. RIOT OS -The friendly Operating System for the Internet of Things. <http://www.riot-os.org/#features> Date of access: 17/12/2015.

Ritchie, D. 2019. LG InstaView ThinQ Refrigerator: A Must-Have Smart Appliance. <https://readwrite.com/2019/09/13/lg-instaview-thinq-refrigerator-a-must-have-smart-appliance/> Date of access: 04/11/2019 2019.

Rosenthal, M. 2016. Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in Pharmacy Teaching and Learning*, 8(4):509-516.

Rowan, T. 2010. Negotiating wifi security. *Network Security*, 2010(2):8-12.

Rush, F. 2006. The Cambridge companion to critical theory: Cambridge University Press.

Rushby, J.M. 1981. Design and verification of secure systems. Vol. 15: ACM.

Sagers, G., Hosack, B., Rowley, R., Twitchell, D. & Nagaraj, R. 2015. Where's the Security in WiFi? An Argument for Industry Awareness. (In. System Sciences (HICSS), 2015 48th Hawaii International Conference on organised by: IEEE. p. 5453-5461).

Samsung. 2015. Privacy. <http://www.samsung.com/za/info/privacy.html> Date of access: 16/10/2015.

Samsung. 2018. NU8000 SMART TV. <https://www.samsung.com/us/support/owners/product/2018-uhd-smart-tv-nu8000> Date of access: 02/04/2019 2019.

SAMSUNG. 2019a. Our approach to privacy. <https://www.samsung.com/us/account/our-approach-to-privacy/> Date of access: 17/09/2019 2019.

Samsung. 2019b. Privacy. <http://www.samsung.com/za/info/privacy.html> Date of access: 16/10/2015.

SAMSUNG. 2019c. Refrigerator User manual for RF22N9781SG/AA (pp. 252): samsung.

Samsung. 2019d. Samsung Developers. <https://developer.samsung.com/tv> Date of access: 21/11/2019 2019.

SAMSUNG. 2019e. Samsung family hub refrigerator. <https://www.samsung.com/us/explore/family-hub-refrigerator/overview/> Date of access: 13/09/2019 2019.

Samsung. 2019f. *Smart TV e-manual* http://downloadcenter.samsung.com/content/UM/201901/20190102114948285/ENG_US_KM2ATSCN-3.0.4.pdf.

Samsung. 2019g. What is Smart TV? <https://www.samsung.com/za/tvs/tv-buying-guide/what-is-smart-tv/> Date of access: 6/11/2019 2019.

SamsungNews. 2017. TV Market Insights: Large Screen, UHD, and Convenience. <https://news.samsung.com/global/tv-market-insights-large-screen-uhd-and-convenience> Date of access: 02/04/2019 2019.

Sathu, H. & Shukla, R. 2007. Home area network: a security perspective. (*In. Proceedings of the 6th WSEAS International Conference on Information security and Privacy (ISP'07) organised by. p. 14-16*).

Saunders, M.N. 2011. Research methods for business students, 5/e: Pearson Education India.

Savvides, A. & Srivastava, M.B. 2002. A distributed computation platform for wireless embedded sensing. (*In. Computer Design: VLSI in Computers and Processors, 2002. Proceedings. 2002 IEEE International Conference on organised by: IEEE. p. 220-225*).

Schlage. 2019. Schlage Sense Smart Deadbolt. <https://www.schlage.com/en/home/smart-locks/sense.html> Date of access: 1/10/2019 2019.

Schneider, D. 2012. The state of network security. *Network Security*, 2012(2):14-20.

Seaman, C.B. 1999. Qualitative methods in empirical studies of software engineering. *IEEE Transactions on software engineering*, 25(4):557-572.

Securityaffairs.co. 2019. 6 Security Flaws in Smart Speakers You Need to Know About. <https://securityaffairs.co/wordpress/73782/iot/smart-speakers-security-flaws.html> Date of access.

Seifert, D. 2019. Google Nest Hub Max review: bigger screen, better sound, and a camera. <https://www.theverge.com/2019/9/9/20855944/google-nest-hub-max-review-assistant-smart-display-price-specs-features> Date of access: 24/11/2019 2019.

Sekaran, U. 2006. Research methods for business: A skill building approach: John Wiley & Sons.

Sen, A. 2017. Your smart TV, fridge could be hacked a lot more easily than you may think. <https://economictimes.indiatimes.com/tech/internet/your-smart-tv-fridge-could-be-hacked-a-lot-more-easily-than-you-may-think/articleshow/61037784.cms> Date of access: 4/11/2019 2019.

Shang, G., Chen, Y., Zuo, C. & Zhu, Y. 2013. Design and Implementation of a Smart IoT Gateway. (In. Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing organised by. p. 720-723).

Sharifi, M., Kashi, S.S. & Ardakani, S.P. 2009. LAP: A Lightweight Authentication Protocol for smart dust wireless sensor networks. (In. Collaborative Technologies and Systems, 2009. CTS '09. International Symposium on organised by. p. 258-265).

Sharma, A. 2019. Top Google Play Store Statistics 2019-2020 You Must Know. <https://appinventiv.com/blog/google-play-store-statistics/> Date of access: 26/11/2019 2019.

Shi, Y. & Lichman, S. 2005. Smart cameras: a review. (In. Proceedings of organised by: Citeseer. p. 95-100).

Silberschatz, A., Gagne, G. & Galvin, P.B. 2018. Operating system concepts: Wiley.

Silberschatz, A., Galvin, P.B., Gagne, G. . 2010. Operating system concepts. 8th. Asia: John Wiley & Sons.

Smarthomeenergy.co.uk. 2019. What is a smart home? <http://smarthomeenergy.co.uk/what-smart-home> Date of access: 14/10/2019 2019.

SmartThings.com. 2019. SmartThings. <https://www.smarthings.com/gb/products/smarthings-hub> Date of access: 19/11/2019 2019.

Smith, J. & Firth, J. 2011. Qualitative data analysis: the framework approach. *Nurse researcher*, 18(2):52-62.

Somani, N.A. & Patel, Y. 2012. Zigbee: A low power wireless technology for industrial applications. *International Journal of Control Theory and Computer Modelling (IJCTCM)*, 2(3):27-33.

Somani, U., Lakhani, K. & Mundra, M. 2010. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. (In.

Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on organised by: IEEE. p. 211-216).

Sony. 2019. Sony privacy policy. https://www.sony.co.uk/eu/pages/privacy/en_GB/privacy_policy.html Date of access: 02/04/2019 2019.

Specht, S.M. & Lee, R.B. 2004. Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. (In. ISCA PDCS organised by. p. 543-550).

Stegener, B. 2018. 7 Ways Alexa and Amazon Echo Pose a Privacy Risk <https://www.makeuseof.com/tag/alexa-amazon-echo-privacy-risk/> Date of access: 25/11/2019 2019.

Stemler, S. 2001. An Overview of Content Analysis. Vol. 7.

Sterling, G. 2019. Survey: 118 million smart speakers in US, but expectation is low for future demand. [https://marketingland.com/survey-reports-118-million-smart-speakers-in-u-s-but-the-expectation-of-future-demand-is-way-down-254937](https://marketingland.com/survey-reports-118-million-smart-speakers-in-us-but-the-expectation-of-future-demand-is-way-down-254937) Date of access: 05/06/2019.

Stewart, J.M., Chapple, M. & Gibson, D. 2012. CISSP: Certified Information Systems Security Professional Study Guide: John Wiley & Sons.

Stragier, J., Hauttekeete, L. & De Marez, L. 2010. Introducing Smart grids in residential contexts: Consumers' perception of smart household appliances. (In. Innovative Technologies for an Efficient and Reliable Electricity Supply (CITRES), 2010 IEEE Conference on organised by. p. 135-142).

Swanson, R.A. & Holton, E.F. 2005. Research in organizations: Foundations and methods in inquiry: Berrett-Koehler Publishers.

Symantec. 2019. Can smart speakers be hacked? 10 tips to help stay secure. <https://us.norton.com/internetsecurity-iot-can-smart-speakers-be-hacked.html> Date of access: 04/06/2019.

Takanen, A., Demott, J.D., Miller, C. & Kettunen, A. 2018. Fuzzing for software security testing and quality assurance: Artech House.

Talos. 2018. Vulnerability Spotlight: Multiple Vulnerabilities in Samsung SmartThings Hub <https://blog.talosintelligence.com/2018/07/samsung-smarthings-vulns.html> Date of access: 25/11/2019 2019.

Tanenbaum, A.S. 2009. Modern operating systems.

Teare, D. 1999. Designing cisco networks: Cisco Press.

Technavio. 2018. 8 Largest TV Manufacturers in the World by Market Share 2018. <https://blog.technavio.com/blog/largest-tv-manufacturers-by-market-share> Date of access: 02/04/2019 2019.

Thestaronline.com. 2018. Chinese smart speaker models prove a hit at home. <https://www.thestar.com.my/tech/tech-news/2018/11/08/chinese-smart-speaker-models-prove-a-hit-at-home/> Date of access: 05/06/2019 2019.

Thomas, D.R. 2006. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, 27(2):237-246.

TinyOS. 2016a. Safe TinyOS. http://tinyos.stanford.edu/tinyos-wiki/index.php/Safe_TinyOS Date of access.

TinyOS. 2016b. TinyOS Overview. http://tinyos.stanford.edu/tinyos-wiki/index.php/TinyOS_Overview Date of access: 25/01/2016 2016.

Tomlinson, P. 2019. Are smart locks safe? Hear what security experts say and check out latest models. <https://www.scmp.com/native/lifestyle/topics/premier-living/article/3006243/are-smart-locks-safe-hear-what-security> Date of access: 29/10/2019 2019.

Trochim, W.M. & Donnelly, J.P. 2001. Research methods knowledge base.

Tsukayama, H. 2017. Smart TV privacy policies: Here's what you're actually agreeing to. <https://www.chicagotribune.com/bluesky/technology/ct-smart-tv-privacy-policies-wp-bis-20170417-story.html> Date of access: 02/05/2019 2019.

Tung, L. 2018. Who's watching your TV? Sony quietly killed three critical Bravia TV bugs. <https://www.zdnet.com/article/whos-watching-your-tv-sony-quietly-killed-three-critical-bravia-tv-bugs/> Date of access: 23/08/2019 2019.

Tyson, P. 1991. Talking about Lesson Planning: The Use of Semi-Structured Interviews in Teacher Education. *Teacher Education Quarterly*, 18(3):87-96.

Uddin, M.F. & Youssef, A.M. 2006. Cryptanalysis of Simple Substitution Ciphers Using Particle Swarm Optimization. (In. 2006 IEEE International Conference on Evolutionary Computation organised by. p. 677-680).

Uehara, M. 2015. The Design of a Framework for Smart Appliances. (In. Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on organised by. p. 457-462).

Urquhart, C.c.u.a.a.n., Lehmann, H.h.l.a.a.n. & Myers, M.D.m.m.a.a.n. 2010. Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems. *Information Systems Journal*, 20(4):357-381.

Vaishnavi, V. & Kuechler, W. 2004. Design research in information systems.

Vaishnavi, V.K. & Kuechler, W. 2015. Design science research methods and patterns: innovating information and communication technology: Crc Press.

Vaismoradi, M., Turunen, H. & Bondas, T. 2013. Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & health sciences*, 15(3):398-405.

Varchola, M. & Drutarovský, M. 2007. Zigbee based home automation wireless sensor network. *Acta Electrotechnica et Informatica No*, 7(1):4.

Vijayalakshmi, A.V. & Arockiam, L. 2016. A study on security issues and challenges in IoT. *Engineering Sciences & Management Research*, 3(11):34-43.

Wagner, S.M., Lukassen, P. & Mahlendorf, M. 2010. Misused and missed use—Grounded theory and objective hermeneutics as methods for research in industrial marketing. *Industrial marketing management*, 39(1):5-15.

Walsham, G. 1995. Interpretive case studies in IS research: nature and method. *European Journal of information systems*, 4(2):74.

Wang, C., Ren, K., Lou, W. & Li, J. 2010. Toward publicly auditable secure cloud data storage services. *IEEE network*, 24(4):19-24.

Wang, H., Zhang, Z. & Taleb, T. 2018. Special issue on security and privacy of IoT. *World Wide Web*, 21(1):1-6.

Weber, R. 2004. The rhetoric of positivism versus interpretivism: A personal view: SOC INFORM MANAGE-MIS RES CENT UNIV MINNESOTA-SCH MANAGEMENT 271 19TH AVE SOUTH, MINNEAPOLIS, MN 55455 USA.

Weber, R.H. 2010a. Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, 26(1):23-30.

Weber, R.H. 2010b. Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1):23-30.

Wetzel, K. 2019. The best smart home hubs for 2019. <https://www.digitaltrends.com/home/best-smart-home-hubs/> Date of access: 19/11/2019 2019.

Willcox, J.K. 2018. How to Turn Off Smart TV Snooping Features. <https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features/> Date of access: 27/05/2019 2019.

Williams, A. 2019. Google Nest Hub Max review. <https://www.techradar.com/reviews/google-nest-hub-max> Date of access: 24/11/2019 2019.

Wohlin, C. & Aurum, A. 2015. Towards a decision-making structure for selecting a research design in empirical software engineering. *Empirical Software Engineering*, 20(6):1427-1455.

Wold, J. 2019. Global Smart TV Market Growth Bolstered by Rising Adoption of OTT Media Services and Consumer Electronics. <http://www.researx.com/smart-tv-market> Date of access: 15/10/2019 2019.

Wollerton, M. 2019. Comparing indoor-outdoor security cameras. <https://www.cnet.com/reviews/arlo-pro-2-security-camera-review/> Date of access: 1/10/2019 2019.

Wortham, S. 2010. Ethnographic research methods. *Education*, 672.

Xiao, L., Greenstein, L.J., Mandayam, N.B. & Trappe, W. 2009. Channel-Based Detection of Sybil Attacks in Wireless Networks. *IEEE Transactions on Information Forensics and Security*, 4(3):492-503.

Xiong, J. & Jamieson, K. 2013. SecureArray: improving wifi security with fine-grained physical-layer information. (In. Proceedings of the 19th annual international conference on Mobile computing & networking organised by: ACM. p. 441-452).

Yale. 2019. Yale Assure Lock SL (YRD 256) with ZigBee. <https://www.shopyalehome.com/products/keyless/YRD256US10BPAssureLockSLwithZigbee.aspx> Date of access: 1/10/2019 2019.

Yan, F., Jian-Wen, Y. & Lin, C. 2015. Computer Network Security and Technology Research. (In. 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation organised by. p. 293-296).

Yan, Z., Qianping, W., Wei, W., Dong, J. & Yiwen, L. 2009. Research on the Priority-Based Soft Real-Time Task Scheduling in TinyOS. (In. Information Technology and Computer Science, 2009. ITCS 2009. International Conference on organised by. p. 562-565).

Yang, B. 2009. Study on Security of Wireless Sensor Network Based on ZigBee Standard. (In. 2009 International Conference on Computational Intelligence and Security organised by. p. 426-430).

Yang, Y., Xia, P., Huang, L., Zhou, Q., Xu, Y. & Li, X. 2006. SNAMP: A multi-sniffer and multi-view visualization platform for wireless sensor networks. (In. Industrial Electronics and Applications, 2006 1ST IEEE Conference on organised by: IEEE. p. 1-4).

Yong, W., Da, R., Dawu, G., Gao, J., Daming, L., Jianping, X., et al. 2011. Analysis of Smart Grid security standards. (In. Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on organised by. p. 697-701).

Zhang, H. & Zhu, L. 2011. Internet of Things: Key technology, architecture and challenging problems. (In. Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on organised by: IEEE. p. 507-512).

Zhao, Z., Huangfu, W. & Sun, L. 2012. NSSN: A network monitoring and packet sniffing tool for wireless sensor networks. (In. Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International organised by: IEEE. p. 537-542).

Zheng, J. & Jamalipour, A. 2009. Wireless sensor networks: a networking perspective: John Wiley & Sons.

Zhu, Q., Wang, R., Chen, Q., Liu, Y. & Qin, W. 2010. IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things. 347-352.

Zigbee.org. 2019. Zigbee 3.0. <https://zigbee.org/zigbee-for-developers/zigbee-3-0/> Date of access: 20/09/2019 2019.

Zotos, K. & Litke, A. 2005. Cryptography and Encryption. *arXiv preprint math/0510057*.