UCLouvain

LOUVAIN
School of Management

Louvain School of Management

Analysis of the Internet of Things in the smart home environment: Context, Challenges and Implications

Authors : Gilles De Buijst & Guillaume Delande
Supervisor(s) : Jean Vanderdonckt
Academic year 2019-2020

FOREWORD

Writing this thesis in such a particular context was a real experience that forced us to adapt quickly to the changing health situation of the country. This challenge taught us a lot and could not have been overcome without the help and support of the people we would like to thank before diving into our work.

First of all, we would like to thank our promoter, Mr. Jean Vanderdonckt, for his trust alongside the great degree of freedom he has given us for our work and for giving us the opportunity to write on such an exciting subject. His references and advices were of great help to us. We would also like to thank our friends and families for the unwavering support they provided us throughout this journey and allowing us to write this work in the best possible conditions. Finally, we would like to express our gratitude to all the people having responded to our survey and everyone who was willing to be interviewed.

Gilles De Buijst & Guillaume Delande

Louvain-la-Neuve, August 2020

ABSTRACT

As the world moves towards digitization, the connectivity of the world as we know it today is growing and will continue to grow in the years to come. A concrete and current example of this growing connectivity in the world around us is undoubtedly the emergence of IoT (Internet of Things) based smart devices in our home environment, bringing with them a new market as innovative as it is complex, which is important to understand for companies wishing to invest in it. In order to achieve this, we have created a Framework based on tools such as a user acceptance model, an online survey and semi-directive interviews, to present the best practices that companies should follow in order to optimize their chances of success in the IoT market and more specifically in the smart home market.

RÉSUMÉ

À mesure que le monde avance vers la numérisation, la connectivité du monde tel que nous le connaissons aujourd'hui s'accroît et continuera à s'accroître dans les années à venir. Un exemple concret et actuel de cette connectivité croissante dans le monde qui nous entoure est sans aucun doute l'émergence des dispositifs intelligents basés sur l'IdO (Internet des Objets) dans notre environnement domestique, apportant avec eux un nouveau marché aussi innovant que complexe qu'il est important de comprendre pour les entreprises qui souhaitent y investir. Afin d'y arriver, nous avons créé un Framework sur base d'outils tels qu'un « user acceptance model », une enquête en ligne et des interviews semi-directives, afin de présenter les bonnes pratiques que les entreprises devraient suivre afin d'optimiser leur chance de réussite sur le marché de L'IdO et plus spécifiquement celui de la maison intelligente.

TABLE OF CONTENTS

APPENDICES

TABLE OF ILLUSTRATIONS

INTRODUCTION

CONTEXT OF THE PROBLEM

As you will be able to see throughout this work, the Internet of Things (IoT) sector and more precisely the 'smart home' trend is in full swing. Following this trend, numerous articles written by experts have been published. These articles often describe the challenges faced by the technology as well as the potential adoption barriers it might be facing. They also highlight the potential that the technology has to disrupt whole industries (e.g. the housing industry).

The reason behind the choice of the topic is very straightforward. Both the IoT and the smart home fields have seen an increase in popularity in recent years. The developments achieved in both fields allow to combine them in order to enhance the quality of services they offer. For instance, a well-designed home automation system, enhanced by IoT technology, can offer multiple advantages such as: automated lighting control, reduced power consumption, improved gardening management, improved home safety and security, better HVAC monitoring, better assistance of disabled and elderly people, and more.

CENTRAL OBJECTIVE

The objectives pursued in this work are multiple. The main objective is to take advantage of the literature, interviews, a user acceptance model and an online survey in order to highlight managerial implications corporate managers should be aware of when wishing to maximize their chance of success. The market is still young and full of innovations, which requires the ability to adapt quickly to changes. It is therefore important to be aware of the different challenges that the market is and will be facing in the future as well as the different solutions companies can already provide and the ones they will be able to provide in the future.

A secondary objective of this work is to see if the different theoretical elements captured through a literature review (e.g. challenges present on the market, early adopter profile, ...) merge with the insights captured through other means (i.e. interviews, acceptance model and a survey).

Furthermore, it was observed that existing literature on managerial implications linked to the IoT-enabled smart home is lacking. Therefore, this work not only aims at gathering the limited existing knowledge but also to close the identified knowledge gap.

As this work aims at providing managerial implications, a final objective of this work is to structure these implications in a framework that can easily be used for practical application.

Assumptions made in this work

In this work, we assume that the reader has already developed some interest in the field of the Internet of Things and more specifically in the smart home sector. We also assume that from this interest some knowledge already flows. As a result, some generic terms may not be defined within this work. However, we do not necessarily assume the reader to be a domain expert. To that regard, the literature review has been structured and written in a manner that should allow the reader to progressively build knowledge on the field. Hence, we believe the literature review to be relatively easy to understand and sufficiently explanatory for anyone to be able to understand the future parts of this work.

Scope of the work and initial limitations

The scope of this work is mainly managerial. Our scope is also quite broad. Indeed, we believe it is interesting to have an understanding of the global IoT market before focusing more specifically on the smart home market. In addition, we acknowledge that the field of DIY IoT devices without commercial intent exist, but we will nevertheless not cover it for several reasons. First due to the vastness of that field and secondly because we believe the managerial implications that can be drawn out of it are rather limited and might not be meaningful at the corporate level.

Throughout this work, we will not go into in-depth technical explanations first because we think that this would not bring much to our goal and could even be detrimental to the reader's understanding and, second, because our knowledge in the fields of IT and Computer Science is rather limited.

Audience

This work is mainly aimed at managers of companies that have embarked on the IoT adventure and, more particularly, the smart home, or who wish to enter this market and are willing to know more about the good practices and areas of interest of customers. However, we also believe that our work can have a more general scope and be of interest to people curious about the future of the home and new connected technologies and who want to be aware of, among other things, the history, the market conditions, the challenges and other implications surrounding the innovative field that is the IoT-enabled smart home. Moreover, several parts in the literature review can be used separately as foundation for other works related to the IoT and/or smart home. For instance, we provide very general definitions for respectively the IoT and smart home, that might be used in other works.

RESEARCH METHODOLOGY

For our research method, we opted for a Traditional Literature Review (TLR) also known as Narrative Literature Review which is a comprehensive, critical and objective analysis of the current knowledge that can be found on a particular topic ("Literature Review: Traditional or narrative literature reviews", 2020).

Onwuegbuzie and Frels (2016) divide TLR in four main categories: the general literature review, the theoretical literature review, the methodological literature review and the Historical literature review. Among the latter, we have opted for the general literature review which aims at providing, among other things, a review of the most meaningful, critical and important aspects of the current knowledge over the topic of interest.

Now that our literature review has been defined, it is also interesting to mention the criteria on the basis of which we have selected our sources. First of all, as we will discuss at the end of the work, in the personal limitation section, since physical libraries were difficult to access, we had to mainly rely on online research and internet sources. To do so, we have favored some platforms namely: Libellule, Google Scholar, Researchgate, IEEE Xplore and ACM Digital Library.

In order to select articles that were interesting and as reliable as possible, we paid particular attention to the following elements. First, the number of citations of the paper when the latter was available. Second, the background of the author(s) both academic and

professional coupled with their past work(s) as well. Third, we also paid attention to the methodology used to write the article. Finally, we also paid attention to the purpose of the research and its expected outcomes.

In order to identify managerial implications, this work relies on an extensive literature review that aims to provide a very broad view of the field. This is done because managerial implications can be drawn from a variety of inputs (e.g. context, challenges, enabling technologies, and more). Then, in order to provide managerial implications that would be in line with the demand side (i.e. users), several means were used to gather insights from a demand side perspective. More specifically, an online survey was conducted with users and non-users of a smart home. Additionally, in order to study users' intention to adopt an IoT-enabled smart home, a smart home-adapted version of the Technology Acceptance Model (TAM) was developed and tested. In addition, qualitative interviews were led in a semi-directive way with smart home users and potential users. More precise information specific to the research methodology is presented after the literature review.

STRUCTURE OF THE THESIS

The structure of this work is divided into two main parts, which are themselves subdivided into several sub-chapters.

The first part consists of an analysis of theoretical elements in the form of a literature review.

This section is composed of four main chapters. The first chapter aims at defining terms that will often come up in the rest of our work. These definitions are our own and have been designed on the basis of popular definitions found in the literature. Once the main terms have been defined, a second chapter will take a look at the context of the emergence of IoT and smart homes. This chapter will allow the reader to learn more about the development of these technologies, discover their origins and understand how they are currently shaping a new context for industries, companies, and people to evolve in. The third chapter of this first part is itself composed of multiple parts. Its aim is to give the reader insights into the IoT and smart home market, to make him/her aware of the complexity of the sector while presenting the various managerial implications related to the development of an IoT-enabled smart

home. In addition, this chapter also covers the main enabling technologies that have forged the identity of the IoT and the smart home so far as well as the many challenges they are facing and will probably continue to face in the coming years. This chapter will ultimately present the most popular solutions to these challenges that are currently promoted in the literature. The fourth and last chapter of this section takes a closer look at user adoption by analyzing traditional models such as the TAM already mentioned above. It will help us identify the different determinants influencing the adoption of the technology.

The second part of this work is the more practical one and is composed of five chapters. We will first explain our research goals. Afterwards, we will go through the description of the multiple tools we used, explain the methodology used, their advantages and disadvantages. The third chapter will highlight our observations and explain how data have been collected and present the first step of the modelling. In the fourth chapter we will highlight the insights we have drawn from both our online survey and our interviews. Finally, we will present our framework that aims at helping corporate managers take meaningful actions to be successful on the IoT-enabled smart home market.

SECTION I - LITERATURE REVIEW

CHAPTER I – DEFINITIONS

A lot of the terms that will be used in this paper have seen various authors trying to define them before, leading to a wide amount of definitions for a same term. Each definition that can be found in the literature has been influenced by the author's specific view, and the article's context and end goals. For instance, the Building Performance Institute Europe (De Groote, Volt & Bean, 2017) defines 'smart homes' as "smart buildings that are flexibly connected and interacting with the energy system, being able to produce, store and/or consume energy efficiently." It can be observed that the scope of this definition is very narrow as it is building- and system-focused and neglects other user needs and services that can be provided by smart homes (e.g. enhanced healthcare at home, more comfort, better security). As with most definitions we've come across in the literature, we consider this definition correct but incomplete. Consequently, it appears sound to propose definitions that take different perspectives into account.

First, we will highlight some of the main definitions declared in the literature, based on the most relevant research and review papers. Then, based on the relevant definitions, we will propose our own definition of the main terms used in this paper.

1.1. IoT

By browsing the literature, an interested reader might encounter a plethora of definitions about the Internet of Things, each bringing multiple novel and different elements. In addition, there is no well-recognized and globally established definition of the IoT yet. Therefore, we decided to synthesize the different elements found in the literature and propose our own definition of Internet of Things.

According to Ashton himself (2009), the phrase 'Internet of Things' was used for the first time in 1999 as a title for one presentation he made at Procter & Gamble (P&G). Ashton observed that computers are heavily dependent on human beings for what concerns information. Indeed, humans capture and create information that is then used by the computer as input. However, humans lack time, attention and accuracy and are therefore not optimal at capturing data about things in the real world. Our environment is based on physical things, not bytes and it is thus crucial to "empower computers with their own means of gathering information about the world." One such example is RFID, that allows "computers to observe, identify and understand the world by themselves, without the limitations of human-entered data." (Ashton, 2009). Rouse (2016) also builds on that idea of limited human intervention and defines the IoT as a system of interrelated components (i.e. computing devices, mechanical and digital machines, objects, animals or people) that have an unique identifier (UID) and that do not require human-to-human or human-to-computer interaction in order to transfer data over a network. Gubbi et al. (2013) denote the requirement to have a unified framework in order to share information across platforms and see the IoT as an "interconnection of sensing and actuating devices". Haller, Karnouskos & Schroth (2009) take a broader view and consider the IoT as "a world where physical objects are seamlessly integrated into the information network." Zhang et al. (2014) help define the meaning of the term 'thing' by associating it with a "physical or virtual object which connects to the Internet and has the ability to communicate with human users or other objects".

The IEEE IoT Initiative (Minerva, Biru & Rotondi, 2015) has also tried to bring up a universally recognized definition of the IoT. This definition is, to our knowledge, the most successful try at defining the IoT. The IoT is defined as "a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture, communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for

anything taking security into consideration" (Minerva, Biru & Rotondi, 2015). While this definition is very complete, it mainly focuses on defining "things" and less on the global picture of a network. In that sense, it does not consider certain aspects of the aforementioned definitions.

While other definitions exist, these ones are the most cited ones, hence common, and offer enough information about the characteristics and components that constitute the IoT. Therefore, we will base our own definition of IoT on a combination of the elements mentioned in these definitions. A summary can be found in the table below.

	Internet				Things				Services						
	Information Network	Internet	Interconnection & intercommunication	Standard communication protocols	Uniquely identifiable	Connectivity components	Physical components	Smart components	Physical / Vertical representation	Ubiquitous sensing	Programmability feature	Anywhere, anytime, by anything	Limited human intervention	Data analytics	Information sharing across platforms
(IEEE Internet Initiative) Minerva, Biru, & Rotondi, 2015		X	X	X	X			X	X	X	X	X			
Haller, Karnouskos & Schroth, 2008	X								X						
Zhang et al., 2014		X	X						X						
Porter & Heppelmann, 2014						X	X	X		X	X				
Gubbi et al., 2013			X							X				X	X
Rouse, 2016	X				X				X				X		
Ashton, 2009									X	X			X		

Table 1 - Summary of the different characteristics and elements composing the IoT mentioned in the literature.

Based on these properties, we propose the following definition for the IoT:

The IoT is an information network of interconnected "things". It is based on the Internet, hence "things" communicate with each other through the Internet, by using standard communication protocols. Those "things" capture and/or process data and exchange them

with the network. "Things" can belong to different management/administrative domains and therefore, an unified framework and standards are required to allow to share information across different platforms. The interrelated "things" can be computing devices, mechanical and digital machines, objects, animals or people, and can be physical or virtual. Those "things" have sensing and/or actuation capabilities, as their goal is to interact with the physical environment. Because humans lack time, attention and accuracy when creating or collecting data on the environment, non-human "things" can be more efficient at those tasks. They empower computers (with their own means) to observe, identify and understand the world. Hence, human intervention (i.e. human-to-human and human-to-computer interaction) is made redundant in the IoT. The IoT creates hereby a need for ubiquitous sensing and actuation devices, data processing and analytics capabilities. Besides sensing and actuation capabilities, "things" also have programmability features and are uniquely identifiable (UID). A "thing" is also versatile as it provides services that are made available anywhere, anytime, and for anything. Most "things" are made of three types of components: smart components (e.g. sensors, microprocessors, data storage, storage), physical components (e.g. electrical and mechanical parts), and connectivity components (e.g. protocols, antennae).

The IoT, because of its limited human intervention and capability to connect a wide number of ubiquitous devices together, creates opportunities for automation, and more specifically home automation in the case of a smart home environment which brings us to our next definition.

1.2. SMART HOME

As for the IoT, multiple definitions of the 'smart home' exist in the literature. They vary in terms of scope and perspective, most of them being more focused on the technological part of a smart home. In this paper we gather the main definitions in the field in order to build our own definition of a smart home, taking into account three main perspectives: technology, services, and user needs.

In terms of the technology perspective, Balta-Ozkan et al. (2013) define the smart home as "a residence equipped with a high-tech **network**, **linking sensors and domestic devices**, appliances, features that can be **remotely monitored, accessed or controlled**, and provide services that respond to the needs of its inhabitants." These specific connected devices, appliances, sensors and actuators are often referred to as 'smart objects' or 'smart devices' in the literature. Galinina et al. (2015) define the **IoT-based smart homes** as "automated buildings with installed detection and control devices, such as air conditioning and heating, ventilation, lighting, hardware, and security systems. These modern systems, which include switches and sensors that communicate with a central axis, are sometimes called 'gateways.' These 'gateways' are control systems with a user interface that interacts with a tablet, mobile phone, or computer; the network connectivity of these systems is managed by IoT." This second definition puts the emphasis on the notion of interaction between the different components of a smart home system (e.g. devices, sensors, central axis, tablets) and network connectivity. Diegel et al. (2005) describe the smart home as a system, enhanced with smart appliances, smart control, smart management, and smart sensors. These four levels of smartness need to **collaborate** in order to create a **smart environment** in the house. This definition takes a broader view on the smart home, identifies the main elements constituting a smart home, and introduces the notion of smart environment.

Besides the technological perspective, it is also relevant to take into account the users' needs as well as the services provided to answer those needs. A substantial part of the literature has been focusing on energy management. Reinisch et al. already noted in 2011 an "awareness and motivation to save energy were existent among homeowners, but that adequate technological support for the users was lacking." Kastner et al. (2005), on their part, noted that building automation systems (BAS) were an almost mandatory condition when building a sustainable (low energy, low emission) home or building. Reinisch et al. (2011) proposed the ThinkHome, a building automation system designed to ensure energy efficiency and comfort optimization. Comfort optimization is important as it "motivates homeowners to employ expensive building automation technology." (Reinisch et al., 2011). Besides increased comfort, more efficient energy management and sustainability, a smart home also allows for peace of mind and reduced operational costs (Reinisch et al., 2011). According to Stojkoska & Trivodaliev (2017), the smart home refers to "the use of ICT in home control,

ranging from controlling appliances to automation of home features (windows, lighting, etc.). A key element of the smart home is the usage of intelligent power scheduling algorithms, which will provide residents with the ability to make optimal, a priori choices about how to spend electricity in order to decrease energy consumption." As already mentioned, the Building Performance Institute Europe (De Groote, Volt & Bean, 2017) requires smart homes to be flexibly connected and with the energy system, for the purpose of more efficient energy production, storing and/or consumption.

Another domain of services of the smart home that has seen abundant research emerge over the years is the one of healthcare services, especially for elderly and disabled people. Demiris et al. (2008) define a smart home as "a residence equipped with technology that enhances safety of residents and monitors their health conditions." The smart home can also be perceived as a means for promoting independent living for seniors (McLean, 2011; Ehrenhard et al., 2014). In that way, McLean (2011) considers smart homes as living spaces that have been deliberately designed to accommodate a variety of interactive technologies, where smart technologies can unobtrusively promote independence. Chan et al. (2008), on their side, define the smart home as "a house, which promises to provide cost effective home care for the ageing population and vulnerable users".

The most complete definition of smart homes from a user needs and services perspective might be the one from Alam, Reaz and Ali (2012). Smart homes are defined as a branch of ubiquitous computing where smartness is integrated into homes for comfort, healthcare, safety, security, and energy conservation. Improved quality of life is made possible by automated appliance control and assistive services. In that sense, context awareness combined with predefined constraints based on the conditions of the home environment, as well as remote control of devices and appliances, allow to improve user comfort. Intelligent monitoring and access control enhance security and safety, and ambient intelligence systems may optimize the household's energy consumption (Alam, Reaz & Ali, 2012). Besides optimizing electricity usage, a smart home can also lead to a better use of the available resources such as water and even result in a reduction of the wastage (Dey, Roy & Das, 2016; Schurgot, Shinberg & Greenwald, 2015). A smart home can also allow to reduce human involvement thanks to its improved monitoring, management, control and automation of the devices connected to the network (Atzori, Iera & Morabito, 2010; Pirbhulal et al., 2016). Yang,

Lee and Lee (2018) denote automation, remote controllability, interconnectedness, and reliability as crucial factors for smart home services.

	Components				Needs and Services					Enablers						
	Sensors	Devices and appliances	User interface	Gateway	Cost efficiency	Security and safety	Healthcare	Quality of life / Comfort	Energy Management and sustainability	Remote monitoring, access and control	Smart management and intelligent algorithms	Ubiquitous computing and ambient intelligence systems	Context awareness	Access control	Automation	Interconnectedness and integrated systems
Balta-Ozkan et al., 2013	X	X								X						
Galinina et al., 2015	X	X	X	X						X						
Diegel et al., 2005	X	X								X	X					X
Reinsich et al., 2011					X			X	X							
Kastner et al., 2005									X							
Stojkoska & Trivodaliev, 2017					X				X	X	X				X	X
(BPIE) De Groote, Volt & Bean, 2017									X							
Demiris et al., 2008						X	X			X						
Alam, Reaz & Ali, 2012		X				X	X	X	X	X	X	X	X	X	X	
Yang, Lee & Lee, 2018										X					X	X

Table 2 - Summary of the different characteristics and elements composing the Smart Home mentioned in the literature.

After reviewing the main definitions and characteristics of a smart home in the existing literature (see Table above), we propose a definition that groups all those characteristics together and takes into account different perspectives. Hence, we propose the following definition:

A smart home relies on a network that allows sensors, actuators, devices and appliances to interact with each other by communicating with a central axis (sometimes called 'gateway') through a specific mode of transmission (i.e. wired or wireless). The central axis' user interface makes it possible for users to interact with it by using their own device, such as a smartphone, tablet, or computer. Smart management and control of these interactions allows to create a smart environment. A smart home environment relies on enabling services and technologies such as remote monitoring, access and control, smart management and intelligent algorithms, ubiquitous computing and ambient intelligence, context awareness, access control, automation, interconnectedness and integrated systems. Together, they allow to: enhance energy management and sustainability, provide better anticipation and response to context, provide better support and assistance to the user's needs, cost efficiency, comfort, safety and security, healthcare, quality of life, and reduced human involvement.

It is also to consider that the existing literature provides different definitions of a 'smart home', depending on the scope given to these two terms. Indeed, both the terms 'smart' and 'home' can be given a different scope. As denoted by Darby (2017), a first category of definitions focuses on the 'home' as "a home, and what it can do for its occupants" while the second category provides a more generic definition of 'home' that includes non-domestic buildings, and focuses on "the building itself – not mentioning occupants at all – and on its connection with energy systems." Hence, some definitions are more home- and user-centric while others are more building- and system-centric.

1.3. HOME AUTOMATION

Very closely related to the notion of smart home is the one of home automation, also called domotics. Home automation refers to the capability to control and automate multiple systems, such as appliances, devices, sensors, and actuators, in the home environment

(Lucero & Burden, 2010). Miori & Russo (2014) define home automation as “the controlling and monitoring of home appliances in a unified system”. Hence, where the smart home rather refers to the environment, home automation refers to the automation of the home network (and its appliances). Home automation is therefore one of the main features of a smart home.

With the emergence of the IoT and more specifically IoT-enabled smart homes, it is easier than ever for devices to communicate with each other. In addition, with the development of other enabling technologies (e.g. sensing technologies, machine learning, Big Data, cloud computing), more opportunities for automation arise. Hence, home automation supports the smart home to deliver value. It is also to note that the level of automation is strongly and inversely correlated to human intervention. Indeed, the more automation in the home environment, the less human intervention is required. That is because home automation services mainly rely on Machine-to-Machine (M2M) communications.

1.4. Wireless Sensor Network (WSN)

Wireless Sensor Networks were not meant to be connected to other systems when originally conceived. However, with the evolution towards the IoT and the opportunities that are created when several devices and systems interact with each other, they have evolved to become more connected. In some way, they can be considered as the predecessors of the IoT-enabled smart home environment and are still part of it.

Based on the literature, we have identified the main elements constituting a Wireless Sensor Network (see Table 3 below). Not all definitions were complete, we therefore propose our own definition of a WSN by gathering the different elements from different sources.

	General	Components			Central station, home sink, home hub, central gateway					
	Network of devices	Wireless communication	Represents a node in WSN	Provides digital interfaces to real-world objects	Collect and store data	Perform local processing	Communicates with the nodes of the network	Communicate with devices outside the home WSN (other environments)	IP address	Proper software manager application
Stojkoska & Trivodaliev, 2017	X	X	X		X	X		X		
Atzori, Iera & Morabito, 2010	X	X	X							
Miori & Russo, 2014	X	X					X	X	X	X
Manrique, Rueda-Rueda & Portocarrero,	X	X	X	X			X	X		
ISO/IEC 29182-2:2013 ('sensor network' definition)	X		X	X			X	X		
Wang et al., 2008		X			X					

Table 3 - Summary of the different characteristics and elements composing Wireless Sensor Networks mentioned in the literature.

Following is our proposed definition of a Wireless Sensor Network:

A Wireless Sensor Network (WSN) is a unified network of devices where each device represents a sensor node in the local network. The devices communicate wirelessly with each other. Those devices capture data about the physical world and forward it to a central station (also called home sink, home hub, or central gateway), that will collect and store the data as well as perform local processing. The home sink communicates with all the (internal) nodes of the WSN. The home sink also has a unique IP address, which allows it to connect to the Internet. Hence, it serves as a connection point to the Internet for the local WSN, which allows the WSN to communicate with devices outside the local WSN (i.e. other environments). Since the home sink is the only device of the WSN that requires an IP address (other devices of the WSN can have one but it is not mandatory), the assigned IP address identifies the entire WSN, and not a single device. To that regard, a proper software manager application needs to be developed on top of the home sink to locate the devices and activate their functions within the

WSN. Connecting the WSN to the Internet allows it to be managed remotely, using a computer, smartphone, or tablet, as well as interact with other devices and systems external to the WSN.

CHAPTER II – CONTEXT OF EMERGENCE

This part will focus on the emergence of IoT-based services and products as well as the recent evolution of smart homes. In order to better understand how and why both the IoT and smart home technologies have emerged over the recent years, it is important to have a look and a global understanding of the context in which they evolved.

2.1 GLOBAL CONTEXT OF THE IOT

The rise of IoT is radically reshaping competition and strategy. However, it is not the first-time information technology (IT) is reshaping these two aspects. Indeed, Porter and Heppelmann (2014) identify IoT as the third IT-driven transformation over the past 50 years. The first wave of IT transformation occurred during the 1960s and 1970s and allowed individual activities of the value chain to be automated. Examples of those automated tasks include order processing, bill paying, manufacturing resource planning and computer-aided design. The second wave of IT transformation corresponds to the rise of the internet. During the 1980 and 1990s the internet allowed for an inexpensive and ubiquitous connectivity, which then led to better coordination and integration across individual activities, geography and with external stakeholders such as suppliers and customers. These two waves fostered productivity and growth by improving the value chain while the product itself remained untouched.

In this third wave, symbolized by the rise of IoT, IT is implemented directly into the product, leading to even greater productivity gains. Small computers are being implemented into products, which enhances interconnectivity. The interconnectivity with other devices and the product allows to collect, store and analyze product data. The data is then used to both improve elements of the value chain such as product design, marketing, manufacturing and after-sale service, and add new elements to the value chain such as security and product data

analytics. In short, the IoT allows to collect product data that is then used to dramatically improve productivity and, in addition, totally reshape the value chain.

1.1. GLOBAL CONTEXT OF THE SMART HOME

Until recently, most smart home systems relied on closed purpose-built Wireless Sensor Networks based on industry-specific standards and that performed their functions independently, without the ability to communicate with other networks (Manrique, Rueda-Rueda & Portocarrero, 2016). While those networks on their own allow for more efficiency and automation inside the home, the overall automation level of the whole environment could be enhanced if those networks and devices were interconnected and interoperable. Challenges related to interconnection and interoperability are assessed in a future part of this work. With the emergence of IoT and the removal of some of its technical barriers, it will is possible to connect a WSN to external devices and networks. Indeed, a WSN's central gateway (or 'sink') can offer a connection point to the Internet. Hence, with the adequate technology, the gateway would be capable of linking the local WSN with other networks and/or devices over the Internet (Miori & Russo, 2014) and the WSN would then become an integral part of the IoT. The bottom line is that, although the WSN was originally conceived as a local, closed, purpose-built network relying on industry-specific standards, WSN applications are now starting to take advantage of the Internet and the WSN is becoming treated as a technology integrated into the IoT ecosystem (Manrique, Rueda-Rueda & Portocarrero, 2016). Adoption of more recent protocols such as the Internet Protocol version 6 (IPv6) should also be favorable to the development of IoT-enabled smart homes.

The smart home is currently shifting towards a more open and interconnected environment - following a holistic IoT paradigm - where devices from different systems are able to interact with each other, leading to an increased level of automation and therefore also reducing human involvement. The IoT is a key driver for that as it allows the multiple devices to connect and exchange data with each other through the Internet.

In the future, it is expected that the smart home environment will rely on more intelligent devices, where predictive technology (i.e. based on machine learning) will be embedded

inside the IoT devices and/or platform and allow the smart home system to be more proactive and anticipate user needs. This will be possible due to the large amounts of data collected and exchanged over the network. Instead of relying only on programmed rules, home automation will then become “smarter” and will also allow for more personalization, as more data will be collected, exchanged and processed.

1.2. Reasons for emergence

Several reasons, mainly technical, may be the cause for the emergence of IoT. Many different reasons have been identified in the literature. However, we will only mention the ones we consider as the main ones.

First, both new and existing technologies supporting the IoT have seen considerable advances in the recent years. Amongst those enabling technologies, advancements in Machine Learning, Data Analytics and Big Data, Cloud Computing and M2M communications can be underlined. Those enabling technologies will be assessed more specifically in a future part of this work.

Second, more and more smart, connected products are being acquired by households. This leads to home environments where sensors are becoming ubiquitous. Therefore, more opportunities for automation are created.

Third, devices need to be able to communicate with each other. Several advances have been made, such as: the emergence of (ubiquitous) wireless connectivity; decreasing rates for data traffic, allowing for high-capacity data traffic; creation of interfaces between network types (middleware), allowing to accommodate multiple standards and formats and leading to seamless connectivity (Saarikko et al., 2017); the development of better protocols such as the more recent Internet Protocol (IPv6). These advances enhance communication and reduce the barriers related to a lack of interconnection and interoperability between objects. Those advances will be analyzed in depth in a later part of this work.

Fourth, components such as sensors, actuators and computers are becoming increasingly smaller in size over time, while improving in terms of processing power and power efficiency (Saarikko et al., 2017; Porter and Heppelmann, 2014). This miniaturization of components leads to smaller, more discrete, and more performant devices in the home environment.

Fifth, since the production of the first hard drive, costs of storing data have considerably decreased. This has led to a constantly increasing volume of data stored (Reinsel, Gantz & Rydning, 2018). In addition, business intelligence tools allow to leverage and extract insights from data much faster than before, as they are increasingly allowing to deal with real-time data. Lastly, new methods have made possible the capture of insights from a variety of types of data (i.e. structured, semi-structured, and unstructured) and from various sources, not only internally but also externally to the company (Gantz & Reinsel, 2011).

Several barriers to adoption of smart homes, different from the aforementioned ones, are being or have already been removed. Please refer to the part concerning the challenges of an IoT-enabled smart home, further in this work.

CHAPTER III - IOT IN HOME AUTOMATION, WHEN OBJECTS START INTERACTING

3.1. Market Overview & Opportunities

The objective of this section is to provide some meaningful figures and statistics to better understand the current and future state of the IoT and smart home market.

In this part, we will adopt a funnel approach. We will first take a look at some key figures about the IoT industry itself and its different areas of application. Afterwards, we will dig deeper into the application we are interested in, namely, the smart home. Finally, from the data we retrieved, we will try to extract a customer profile in order to determine the target audience that is most susceptible to adopt the technology and drive its future.

Before going into the market analysis here are some preliminary remarks about the methodology adopted. The statistics and data provided in this section comes mainly from reports published online by Growthenablers for IoT data and from Statista for smart home data. When possible, these data have been cross-checked with other sources to ensure their

accuracy. Finally, to ensure consistency, data in USD had to be converted into EUR. For this purpose, the average exchange rate for the year concerned was used.

3.1.1. INTERNET OF THINGS

In a report published in 2017, Growthenabler first points out that the IoT market is growing. Indeed, this market represented €141.91 billion back in 2016 and could be worth more than €406.75 billion by the end of 2020. This development would therefore obviously also have an impact on IoT connections, which are meant to increase at a CAGR[1] of 16%, from €5.42 billion in 2015 to €24.4 billion by 2025.

Moreover, in terms of investments, the IoT is still the vector of many hopes. Indeed in 2016, the global IoT industry attracted €4.03bn in funding. Looking ahead, the worldwide fundings are still expected to grow at a healthy rate of 5% each year. In addition, in a report published in 2013, Cisco highlights that only 0.06% of the objects that could be connected to the internet currently are, leaving plenty of room for innovation (Cisco Systems, 2013, p.2).

The IoT market can be broken down into several sub-categories that are sharing the market. The sectors sharing the largest share of the IoT cake (projection made in 2017 for 2020) are presented in the following table:

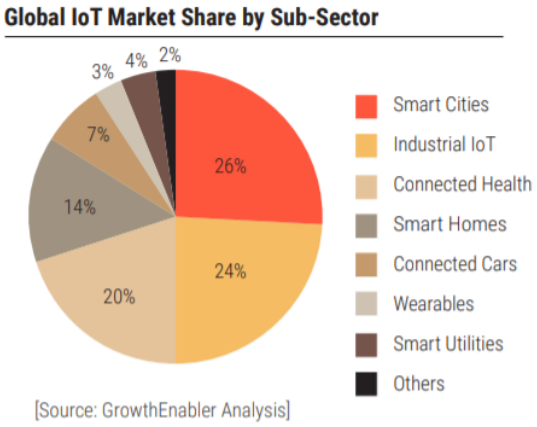


Fig. 1 - Global IoT Market share by Sub-Sector (GrowthEnabler, 2017).

[1] Compound Annual Growth Rate

A last, worth mentioning, information is the spendings on IoT security as we will analyse it more carefully later on. According to a study conducted by Gartner in 2018, the spendings on IoT security reached €1.27 billion in 2018 and are expected to amount to €2.63 billion in 2021 as scientific often predicts security to be the main obstacle for mass IoT adoption (Gartner, 2018).

3.1.2. SMART HOME

Let's now narrow down on the smart home sub-category.

Let's first go through the scope of the data selected for this part. Considered are devices that are connected directly or indirectly via a gateway to the Internet. Their purposes are mainly the monitoring, control and regulation of the environment of a private household. Devices whose primary function is not the automation or remote control of household equipment are not included. Similarly, devices that relate to household connection and remote control only to a limited extent, such as smart TVs, are not included either (Statista, 2019).

According to a report published by Statista, the revenue generated by the smart home industry amounts to €80,563 million in 2020. With a projected CAGR between 2020-2024 of 15%, the market volume is expected to skyrocket and exceed the €140.000 million mark by 2024. In september of 2019, the revenue was mainly generated in the United States of America (€24,486 million) followed by China (€18,500 million) and Germany (€4,272 million).

When taking a look at the household penetration of the technology, another trend is emerging. In fact, the countries where the penetration is the highest are the United States of America (32,4%), Norway (30,5%), Sweden (28,5%), Denmark (27,4%) and South Korea (26,5%). Northern Europe thus seems to be a cluster of early adopters of the technology.

Another meaningful data to take a look at is the revenue generated in each sub-sector of the smart home and their revenue growth both currently and in the future. The smart home is usually divided into six main market segments.

1. Smart Appliances with 23,65% of the total market share and a growth rate of 26,79% in 2020.
2. Control & Connectivity 23,24% of the total market share and a growth rate of 23,32% in 2020.
3. Security with 21,38% of the total market share and a growth rate of 22.22% in 2020.
4. Home entertainment with 13,49% of the total market share and a growth rate of 17,24% in 2020.
5. Comfort & Lighting with 10,17% of the total market share and a growth rate of 26,18% in 2020.
6. Energy Management with 7,99% of the total market share and a growth rate of 24,51% in 2020.

According to projections, this ranking is about to change. In 2024, the revenue generated by security applications will reach second place with a market share of 22,40%. In addition, the comfort and lighting applications are expected to take sole position of fourth place thanks to a market share of 12,28%.

3.1.3. EARLY ADOPTER AND CUSTOMER PROFILE

According to data from Statista, the typical customer who would be most likely to adopt a smart home would be a man (57%) living in the US (32.4%) or Northern Europe (28.8%) aged 25 to 34 (33%) and living on a low[2] (42.4%) or medium[3] (31.3%) income.

This constitutes a great news for the IoT sector and particularly for the smart home industry because, according to a study conducted by Ritholtz (2018), the fastest growing age group of new homeowners are millennials. In addition, millennials have grown up surrounded

[2] 0 - 1270€ after taxes in 2017 according to Insee ("Pauvres, moyens et riches ? Les revenus par type de ménage", 2020)

[3] 1271€ - 2297€ after taxes in 2017 according to Insee ("Pauvres, moyens et riches ? Les revenus par type de ménage", 2020)

by new technologies and value connectivity sometimes more than other "house features" (Ritholtz, 2018).

3.2. FUNCTIONING OF A TYPICAL IOT DEVICE IN A SMART HOME ENVIRONMENT

3.2.1. OVERVIEW

Before going further and take an in-depth view on elements of the IoT and home automation, it is important to take a more holistic view and identify the different elements constituting the IoT landscape. Minerva, Biru, & Rotondi (2015) have identified the following elements related to the technological and social aspects of the IoT:

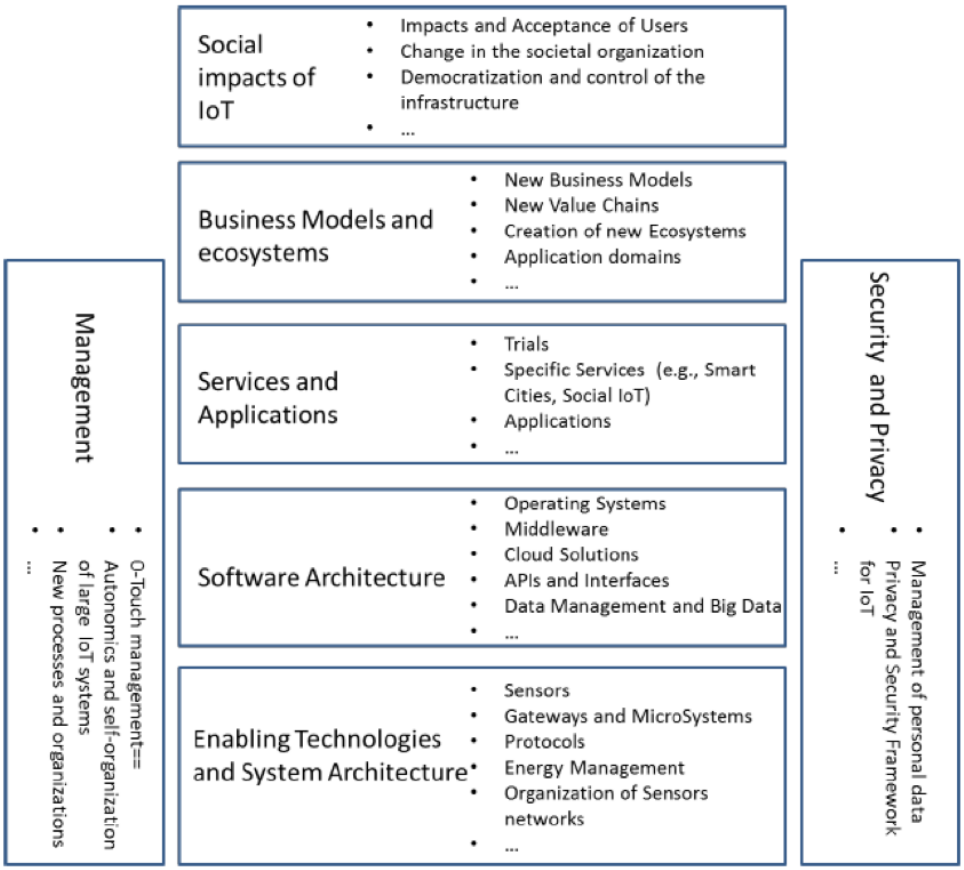


Fig. 2 - Technological and social aspects related to IoT. (Minerva, Biru, & Rotondi, 2015).

3.3. ENABLING TECHNOLOGIES

As already mentioned earlier, the IoT and its application in home automation cannot be considered as "standalone" technology. Many breakthroughs and advances in various fields such as telecommunications, informatics, electronics and even social science have allowed the emergence of IoT and home automation as we know it today (Atzori, Iera & Morabito, 2010). These enabling technologies continue to be developed and may continue to further impact the development of smart homes and the IoT in general. It is therefore important to have them in mind when thinking about the future of home automation. Therefore, we felt it was essential to devote a part of our work to it.

The following list is non-exhaustive, we have tried to include the main technologies that have, have had and will have a real impact on the IoT paradigm and more precisely on the smart home sector.

3.3.1. IDENTIFICATION, TRACKING AND SENSING TECHNOLOGIES

Important advances in nanotechnologies and miniaturization have enabled the reduction in size, weight, energy consumption and cost of the various sensors and actuators (van Dijk & Teuben, 2015). These advancements have played an important role in the development of connected objects. Indeed, these advances have made it possible to integrate sensors and actuators into almost all devices that can be found in a house, regardless of their size and energy consumption (Atzori, Iera & Morabito, 2010).

In terms of identification and tracking, the Radio-Frequency IDentification technology (RFID), invented in 1948 by Harry Stockman, has been a real pillar for the IoT and has contributed to create the IoT paradigm (Advanced Mobile Group, 2015).

RFID is a technology-based identification system which helps identifying objects just through the tags attached to them, without requiring any light of sight between the tags (microchip attached to a small antenna) and the tag reader (scanner with antennas). All that

is needed is radio communication between the tag and the reader and a processor/controller which receives the reader input and process the data (Elprocus, 2020).

Another technology that forged the IoT are Wireless Sensor Networks (WSNs). Wireless Sensor Networks have already been defined in the first chapter of this part, please refer to it for more information.

In the future, the field of biometrics holds a lot of promises for the IoT and the connected home. The Merriam-webster dictionary defines the field of biometrics as "everything related to the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity" (Merriam-Webster, 2020).

As we will see in more detail in the "Challenges" section, the security of connected objects within a smart house is a crucial element for mass adoption of the technology. As a result, many biometric applications could come to meet this craving need for security and more particularly the need for identification and access control. They could ensure the integrity of the data managed by the objects. This would be an important step towards mass adoption by solving a major challenge.

3.3.2. SMARTPHONES AND MOBILE COMMUNICATION TECHNOLOGIES

As we have seen it in our IoT definition, An important promise of the IoT paradigm is the following: “Granting people and things to be connected any-time, anyplace, with anyone, ideally using any network and any service” (Gunge & Yalagi, 2016).

To keep that promise alive, the Internet of Things relies on the advancement made in the smartphone industry and in the field of mobile communication technologies.

On the one hand, the smartphone has enabled us to be connected to the internet and its functionalities anywhere, at any time (Dey, Roy & Das, 2016). On the other hand, the mobile communication technologies and protocols such as Bluetooth, IEEE 802.11 (Wifi), Zigbee, 5G... have enabled objects to communicate and share data with each other (Dey, Roy & Das,

2016). When put together, these two enabling technologies are at the basis of the IoT paradigm and allows it to meet its objective.

3.3.3. CLOUD COMPUTING, DATA ANALYTICS AND BIG DATA

Big data and cloud computing are two terms that are often confused. Let's start by looking up the definition in the Oxford dictionary:

The term big data refers to “extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions” (Lexico, 2020).

Whereas cloud computing refers to “the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer” (Lexico, 2020).

The utilization of smart devices and sensors are generating enormous amounts of data, often exceeding the capacity of a local server (4.4 trillion GB projected by the end of 2020) (Oracle, 2015). With the generation of this enormous amount of data, cloud computing is playing a significant role in the storage and management of that data. Cloud computing service providers such as Microsoft (Azure), Amazon (AWS) or Google (Cloud platform) are providing adequate performance and scalability to store and operate such a huge volume of data and also facilitate its navigation through the use of the internet (Dey, Roy & Das, 2016). In addition, according to whizlabs, “IoT devices which utilize common APIs and back-end infrastructure can receive important security updates instantly through the Cloud as soon as any security breach happens in the infrastructure” (Verma, 2018). This IoT and Cloud computing combined feature is a vital parameter for user security and privacy. Moreover, the International Data Corporation (IDC) projects that in 2023, “more than 90% of all IoT data will be hosted on service provider platforms as cloud computing” (Banafa, 2018), which highlights the importance of cloud computing in the field of the Internet of Things.

Once the data is stored, the advancements made in the field of big data enables the device and sensor-generated data to be fed to a big data system for analysis that produces final reports out of it.

The convergence of the IoT, big data and cloud computing can provide new opportunities and applications in many different sectors including home automation and smart buildings.

To sum it all up, “recent advancements in cloud computing and data analytics allow intelligent systems to store, process and analyze the data in a more efficient manner.” (Dey, Roy & Das, 2016).

3.3.4. GESTURE-BASED CONTROL

During this last decade, the research in the gesture-based control and Human-to-Machine communication (H2M) fields has been flourishing. These advancements in research have been partly due to the widespread of IoT devices coupled with the trend towards smart housing. Some devices such as Microsoft’s Kinect have even inspired novel ways of interacting between humans and machines (Mohammed et al., 2016).

In recent years, the way humans and machines are interacting has changed drastically. The relationship we have with our home devices and appliances has greatly changed due to their growing connectivity, communication capabilities and interactions. At the same time, many advances have been made in human-machine communications, making it even more pleasant to share moments of our lives together. These advances in gesture-based control could make the use of connected objects even more straightforward and convenient (Dey, Roy & Das, 2016).

A striking example was the creation of the Myo armband back in 2014. The objective was to create a new type of human-computer interface through the use of a connected armband that lets you control practically any electronic devices through hand gestures and motion (Bloomberg, 2014). Unfortunately, its production has stopped in 2018 (Myo Team, 2018).

3.3.5. VOICE-BASED CONTROL

Like most of the technologies developed in this section, the field of voice-based control has undergone lots of major innovations and upgrades in recent years. Several large multinationals have embraced the voice-based control hype by creating their own virtual assistant allowing customers to remotely control more and more objects thanks to their voice. Some worth mentioning companies are Google with its Google Home, Amazon with Alexa or Samsung with Bixby. As the performance and accuracy of speech recognition continues to increase, its applications in the connected home are likely to explode in the coming years (Serrenho & Bertoldi, 2019).

3.3.6. MACHINE LEARNING

In recent years the field of machine learning has developed enormously mainly due to the strong willingness of many companies to adopt this trendy technology, even though more traditional data analysis, could in many times do the job.

Nevertheless, in the field of IoT, it's often “necessary to identify correlations between dozens of sensor inputs and external factors that are rapidly producing millions of data points” and this is where machine learning excels at. Moreover, the predictive capability provided by this technology can also have a crucial impact on connected objects (McClelland, 2017).

Indeed, as we are already witnessing today, thanks to companies such as Netflix and Amazon, machine learning is being used to learn more about our preferences. The application of machine learning in the IoT field can therefore be extremely valuable in order to adapt our environment to our preferences and maximize our comfort (Smith & Linden, 2017).

A striking example of the application of machine learning in the Internet of Things and, more specifically, in home automation is the Google Nest Thermostat. That smart device uses machine learning to determine the heating preferences of the inhabitants and adapts the inhouse temperature accordingly throughout the day (McClelland, 2017).

The union between IoT and machine learning is still in its infancy, but there is undeniable evidence that many applications will emerge thanks to the union of these two technologies, the possibilities are infinite.

3.3.7. GAMIFICATION

As we already witnessed in the "*Market Overview & Opportunities"* part, growth projections in the IoT and smart home fields are expected to be very important. As a result, significant competition in these sectors is already present and will certainly be even stronger in the future.

In such context, it is important for companies to differentiate themselves from others. One way to differentiate themselves is to provide customers with unique, meaningful and rewarding experiences as mentioned in the twelfth managerial implication. These experiences result in increased consumer engagement, conversion and loyalty (Fuhriman, 2015).

Gamification is one of the preferred means of providing this experience. Gamification can be defined as "the process of using game mechanics and game thinking in non-gaming contexts to engage users and to solve problems. Gamification leverages game design, loyalty program design and behavioral economics to create the optimal context for behavior change and successful outcomes." (Engagement Alliance, 2020).

According to Jeff Fuhriman, former senior manager in digital marketing at Adobe, gamification can increase consumer loyalty and engagement through the use of three unique gamification-specific abilities. The ability to encourage real-time interactions, the ability to enrich the social engagement, and finally, the ability to rewarding loyalty in an entertaining way (Fuhriman, 2015).

All these elements are showing that gamification is worth keeping an eye on when thinking about the future of the Internet of Things and the smart home particularly because it is a way for companies to get ahead of competition.

3.4. CHALLENGES (CONCERNS, POTENTIAL IMPACTS AND SOLUTIONS)

As we have seen in the previous sections, the IoT seems to be strongly growing and the statistics for its adoption seem to be encouraging, as are the new connected objects that are being created every year. Whilst the predictions seems to predict a flourishing future, everyone agrees that the IoT in the smart home environment is still subject to many different challenges that, if not overcome, could suddenly impact this great development perspective (e.g. Atzori, Iera & Morabito, 2010; Pirbhulal et al., 2016; Wurm et al., 2016).

The objective of this section is to present the main different challenges that the IoT is currently facing, present their potential impacts and propose some solutions that we have been able to find in the literature.

3.4.1. SECURITY

Numerous studies agree that security is one of the most, if not the most, important challenge for mass adoption that the IoT and its application in the smart home are currently facing. All IoT devices with computation and communication capabilities should be considered as interesting and as accessible gateways for hackers to compromise the security of the entire household network and all objects that are connected to it (e.g. PCs, mobile phones, smart objects,...) (Atzori, Iera & Morabito, 2010).

We will first analyze and explain the different types of security requirements that the IoT must meet to reach mass adoption and decrease concerns. This will help us understand what is at stake and witness the complexity of the challenge. We will then explain why IoT devices are particularly prone to attacks, review some of the most popular types of attacks that are actually possible to be carried out on IoT devices, explain what they consist of and finally, depict their effects.

3.4.1.1. Security Requirements

According to an article published by Pirbhulal et al. (2016), the different security factors that the IoT needs to meet can be fractionated into two distinct categories: on the one hand,

everything that is related to data security and, on the other hand, everything related to the network security. Let's first take a look at the data security elements:

- The first data security requirement is **confidentiality** which is also highly linked to the concept of privacy that we will discuss in more details later. The principle of confidentiality is based on the idea that the information transmitted must be protected from disclosure. In the field of IoT as well as in the smart home context, the data transmitted are numerous and it is essential that they are not captured by neighboring or external networks that could seek to use them for malicious purposes.

- Another requirement is **data integrity**. This means that in a secure system, it is important to be able to check whether the transmitted data has not been modified during its journey from the source node to the destination node.

- The last security requirement related to data security is **data freshness**. This principle aims at protecting the user from attackers that may want to capture the data transmitted by the connected devices inside a network and replay it later on, on the same network. It thus implies that the data received by the destination node is novel and not just a replica of a previous data exchange.

Moving on to the network security section:

- The first requirement is **authentication** which, as its name suggests, deals with issues such as identity theft. The presence of multiple smart devices communicating remotely with each other within a network is often an excellent entry point for attackers. The principle of authentication is fundamental and ensures that the information transmitted to the destination node actually comes from a system identified source node and not from an ill-disposed or malicious third party standing outside of the system.

- The second element, closely linked to authentication, is (third party) **trustworthiness** which consist of ascertaining trust to a third party that has been identified beforehand. As explained by Pirbhulal et al. (2016), a third-party trust is a situation in which the source and destination nodes have not established communication path for data transmission before but are nevertheless able to implicitly trust each other. An example of third-party trust is provided by Truong et al.: "entity A trusts entity B because B is trusted by entity C. In this example,

entity A derives trust of B from C, and A also trusts entity C does not lie to him." (Truong et al., 2016, p.2).

- "**Secured Localization**" is the third network requirement. Knowing the exact location of the source of data transmission in a vast network composed of multiple sensor nodes is key. If secure localization of the data source is not ensured, the attacker could transmit incorrect information about the source location by stating fake signal strengths.

- A fourth network requirement is **non-repudiation**. Non-repudiation is the principle according to which nobody can deny the validity of an action from the source node. A broader and telling example of non-repudiation can be found in digital signatures. Indeed, digital signatures ensure the principle of non-repudiation in online transactions where "it is crucial to ensure that a party to a contract or a communication can't deny the authenticity of their signature on a document or sending the communication in the first place." (Cryptomathic, 2020).

- The fifth requirement concerns the **availability** of the system's resources. This condition implies reliable and rapid access to system resources for all sensor nodes inside the network.

- The sixth and last network requirement is called **access control** and is one of the most important principle that needs to be ensured in IoT applications. The main idea behind this principle is that we need to be able to recognize each user and device inside a given network in order to apply security policies specific to each of them. According to Daniel Crowley, a data security specialist and head of research for IBM's X-Force Red, access control thus relies on the two principles of authentication and authorization (Martin, 2019).

This access control principle allows, among other things, the implementation of processes such as the network access control (NAC) which is capable of blocking or limiting access to the network to unidentified sensors or users (Pirbhulal et al., 2016).

Now that all the security requirement have been presented and quickly explained let's move on to the next section that is trying to highlight the main reasons why IoT devices currently suffer of important security breaches.

3.4.1.2. An overview of the root causes of the vulnerabilities

One of the reasons why security has become a major problem today in the smart home field is related to the rapid development of the Internet of Things and Cyber-Physical Systems (CPS)[4] coupled with the production policy adopted by many companies on the market. Indeed, this important development induces a very short time to market (TTM) as well as a need to reduce the production costs of devices both in terms of design and development (Wurm et al., 2016). The desire to benefit from the first mover advantage also pushes manufacturers not to consider, or at least to consider only at a later stage, the security issues of the devices they produce. Other vulnerabilities, attributable to the manufacturers and resellers, are highlighted by Mark Stanislav & Zach Lanier during their presentation at Def Con 22. Amongst those are the support accounts resellers provide for updates and remote support that all share the same password, the default password that is never changed by the customer and the security issues in the software application used to command the IoT device that could jeopardize the whole household network integrity.

Another reason, linked to the first one developed above, is the lack of hardware level security methods. Indeed, attacks on connected systems can mainly take three distinct forms. They can either happen on the hardware level -the physical parts of the system-, the software level, or may even be directly attacking the network (Wurm et al., 2016).

As explained by Wurm et al. (2016) in their paper entitled "Security Analysis on Consumer and Industrial IoT devices", the few security solutions implemented in connected devices are often implemented after the object itself has been manufactured and only offer insufficient software-level protection schemes. According to them, these protections do not consider the inherent specificities of connected objects while implementing solutions and adopt similar solutions to those used on embedded systems or PCs. Hence, these solutions are often implemented by leaving the hardware unintentionally vulnerable.

---

[4] As defined by Monostori (er-Physical Systems (CPS) are systems of collaborating computational entities which are in intensive connection with the surrounding physical world and its ongoing processes, providing and using, at the same time, data-accessing and data-processing services available on

As mentioned in the previous paragraph, specific solutions for connected objects are necessary in order to take into account their inherent specificities. First of all, connected objects spend most of their time unattended, which makes them vulnerable to physical attacks (Wurm et al., 2016; Atzori, Iera & Morabito, 2010). Second, IoT devices are still characterized by reduced capacities both in terms of energy, computing resources, range of communication and memory. These limitations makes difficult and limit the implementation of complex security mechanisms such as asymmetric encryption algorithms that would be too resource-consuming (Atzori, Iera & Morabito, 2010; Ghayvat et al., 2015; Pirbhulal et al., 2016). Therefore, as pointed out in Pirbhulal et al. (2016), a "highly secured IoT based smart home systems which could provide a balance between level of security, energy-efficient security algorithm implementation based on efficient key generation mechanism for data encryption, and capability of network to support communication among large number of IoT nodes at wide coverage range is much needed.".

3.4.1.3. Different types of cyber attacks

As explained in the previous point, attacks can be operated at 3 different levels: hardware, software and network. We will therefore present the most frequent attacks using these categories. The objective is not to go into the technical specifications of the attacks but to understand their basic way of functioning and their potential impact. Please note that for these attacks to be successful, the device targeted must have at least some computation and communication capabilities.

At the hardware level, we will not enter much technical details as the intern structure of devices can vary. Moreover, the objective here is not to develop a secure IoT device but to become aware of the different vulnerabilities specific to IoT devices. A more technical analysis would be outside “the managerial” scope and objective we established for this work.

Hardware attacks often start with a reverse engineering phase. During this phase, having direct access to the device is necessary in order to discover the different elements that compose the hardware. The main goals are to determine the Operating System (OS) under which the device operates and to determine if any machine interfaces are available to gain access the shell (user interface of the operating system). Once such an interface has been

discovered the goal is to find the root or administrator password in order to take control of the device. Various techniques can be used such as brute force attacks or dictionary attacks. Once the password is discovered, the device is completely compromised and can, in some cases, even be remotely exploited. Having access to the code governing the operation of the device, it is also possible for an attacker to inject a malicious program to attack other nodes in the local network and thus, compromising other objects connected to it.

Moving on to the software level, the most prevalent attack is the ransomware. The functioning of a ransomware attack is very simple. The attacker uses malware to encrypt his victim's personal data. Once the operation is done, the attacker will ask for a certain amount of money without which he will not decrypt the data. Moreover, paying this ransom never guarantees that the victim will ever get his/her data back.

At the IoT level and especially at the connected home level, such attacks can be disastrous. A concrete and mind-blowing example was provided by two employees of PenTestPartners, a penetration testing company and security service provider, at the IoT village during Def Con 24. They created a fully functional ransomware that attacks a smart thermostat, allowing them to set and lock the temperature until they get paid (Tierney, 2016).

At the network level, two different types of attacks will be tackled. First, the Distributed Denial of Service (DDoS) attack. This kind of attack is different from the others because its primary objective is neither to steal nor to modify data. Indeed, its goal is to deliberately attempt to cause a capacity overload in the system by sending a high number of requests in a limited time period. This overload of request is capable disabling a service and could compromise the status information of the smart home devices (Ali & Awad, 2018). Examples of this type of attacks are numerous, from shutting down a smart fridge to shutting down connected wearables, the possibilities are endless. In order to make these DDoS attacks, attackers make use of what is commonly called botnets which basically are “a string of connected computers coordinated together to perform a task” (Norton, 2020). The most popular botnet that was used to conduct DDoS attack on several IoT devices was called Mirai. It has infected an estimate of 2.5 million smart devices and used them to shut down other IoT devices. To gain control on the 2.5 million devices, hackers only had to scan the internet for

IoT devices and attempted to log in the default passwords (Fruhlinger, 2018). This brings us back to the issue, already mentioned previously, that Mark Stanislav & Zach Lanier pointed out at Def Con 22 about not changing the default password of a connected device. In addition, prior to the IoT and connected devices, hackers had to use botnets composed of computers to launch a consistent DDoS attack. Now, as the example of the Mirea botnet shows, they simply have to take control of millions of connected devices to make their attacks successful (Ungureanu, 2016).

The second type of network-based attack is the "Man-in-the-Middle" (MiTM) attack and can also be found in the literature under the name of proxy attack. The main principle of this attack is the following: an attacker penetrates the communication channel between two particular systems with as main objective: the interception of the communication between them. As a consequence, the two parties believe that they are directly communicating with each other but all the data they communicate transits through the attacker first. For further explanation of this attack, we based ourselves on a figure provided by (Atzori, Iera & Morabito, 2010).

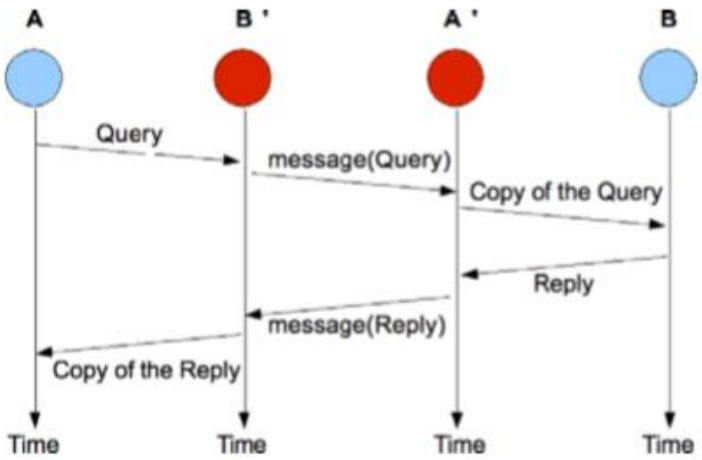


Fig. 3 - Diagram of a typical MiTM attack provided by Atzori, Iera & Morabito (2010).

In a situation in which A is the source node that wants communicate through some wireless mechanism to a destination node B. An attacker that wants to intercept the data transmitted

between A and B will take the identity of the element B (with B being any IoT device). To do so, the attacker will first simulate an access point to which element A will have to connect. Once A is connected, the attacker will position two transceivers (A' and B'). These transceivers will make A believe that B' is B and reciprocally, make B believe that A' is A. All the data transmitted between A and B will transit through the hacker thanks to the transceivers and the victim will not even notice its presence as all the queries send by A will be answered by B'. This can be done regardless of whether the signal is encrypted or not.

Now that the main hardware, software and network attacks have been covered, it is also important to be aware that attacks can take place at several levels. This is the case of attacks called Advanced Persistent Threats (APTs). These attacks use several software and network methods developed above with the objective of gaining a long-lasting access to a system in order to continuously steal private information by staying undetected.

Kaspersky (2020) divides this kind of attack in five steps:

1) Gaining access to the system thanks to an infected file, junk email, or an app vulnerability to insert a malware on the user's network.

2) Establishing a foothold by installing the malware that will create backdoors and tunnels to move around in the system while staying undetected.

3) Deepening the access by trying to acquire administrator rights to have even greater level of control.

4) Moving laterally by trying to infect other servers and secure parts of the network.

5) Look, Learn, and Remain

These attacks are often targeted at high value targets by utilizing social engineering methods such as spear phishing.

Some types of attacks cannot be classified into the aforementioned categories. This is the case of Social Engineering. This is a generic term used to describe malicious activities carried out thanks to human interaction. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information (Imperva, 2020). Such attacks are

hardly attributable to the manufacturer or reseller of the attacked product because the attack is not based on product vulnerabilities but on mistakes made by the users themselves. According to Imperva (2020), these attacks can take several forms but usually follow the same 4-steps pattern.

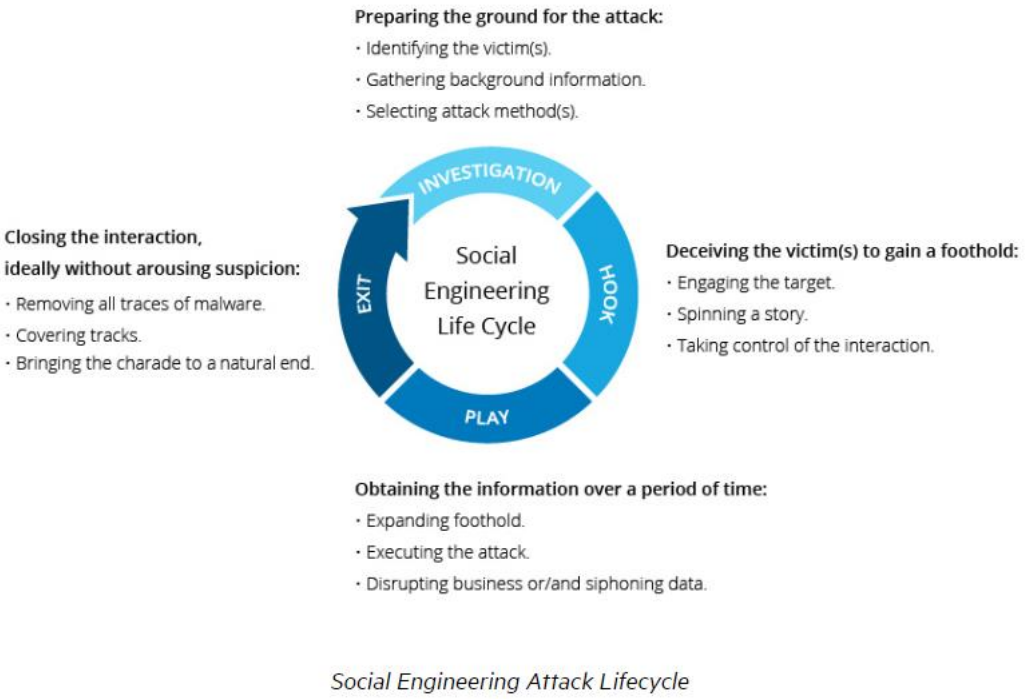


Fig 4. - Social Engineering Life Cycle provided by Imperva (2020).

Amongst the well-known forms of attacks in this category, phishing is probably the most popular one. Phishing can be described as the practice of sending a message to the potential victims with the aim of intriguing or panicking them. Once this psychological situation is reached, the attacker will push them to reveal personal information or click on links containing malwares. A more advanced type of phishing is called spear phishing, which attacks individual that have been identified beforehand. The messages sent are highly personalized, which makes the attack less suspicious and increases its success rate.

Another attack that is using social engineering methods is baiting. Its specificity is that it can come from the physical world as well as from the digital world. In the physical world, the attacker could drop a bait such as a USB stick near the victim. Out of curiosity, the victim will

pick it up and will plug it into their home or work computer and gets infected by a malware. In the digital world, baiting often takes the form of an eye-catching advertisement aimed at making the victim download malicious files.

Finally, the last type of attack that will be discussed in this section about social engineering is called "scareware". This attack consists in flooding the victim with alerts such as the widely spread "your computer is infected contact us as soon as possible" in order to make him/her get in touch with a call center. Employees of that call center will remotely take the control of the victim's PC thanks to software such as TeamViewer in order to steal valuable information such as their bank account credentials.

With the ever-increasing number of connected devices such as wearables, collecting ever-larger volumes of Personally Identifiable Information (PII), a security flaw in one of these could disclose an important amount of personal information to the attackers. These PII would then allow attackers to carry out their malicious activities such as spear phishing much more easily than before.

This brings us to the end of the analysis of the first major challenge that the IoT and the technologies related to the smart home are facing.

3.4.2. PRIVACY

The second important challenge to which connected devices must respond to is that of data confidentiality and privacy in general. Between the information disclosed by WikiLeaks, the Facebook-Cambridge Analytica scandal or the data breach that affected Heartland Payment Systems back in 2009, data breaches seem to be multiplying over the years worrying both companies and individuals who see their private data published online for all to see. Throughout this part, we will define what privacy in the online context is, why it is a particularly difficult challenge to overcome in the IoT paradigm and the potential impact that the lack of privacy in connected devices could have on a smart house owner.

As privacy is a social concept that aims at protecting personal information, the definition of personal data may vary amongst different people because they would value it differently

according to their personal values and beliefs. Nevertheless, thanks to the General Data Protection Regulation (GDPR) published in 2016 and applicable since 2018, the European Union now has an official definition of personal data that has been created in the light of digitalization and particularly the emergence of the IoT.

It is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (gdpr-info.eu, 2018, Art. 4).

Under the IoT paradigm every object that can be connected will be connected. The result of that internet connection is a tremendous quantity of data distributed by these objects. The data produced by each one is valuable for companies as it reveals more about its users' habits and potential preferences. Certain characteristics of IoT devices make the challenge of privacy even more complex. First of all, as Mark Stanislav points out at Def Con 22, an IoT device probably has 3 or 4 services behind it provided by 3 or 4 other vendors, so it's extremely hard to know where your data is going to end up. The customer often finds himself in a situation where he has to blindly trust the person who created the hardware and hope that the manufacturer has a good service provider on the back end. Another element that makes privacy difficult to maintain is the ever-decreasing cost of information storage[5] leading to a situation where the data gets retained forever. In addition, due to the numerous occasions for personal data to be collected by IoT devices, it will become impossible to personally control every piece of information we disclose. Finally, if we broaden our scope to, for instance, smart buildings where numerous people would work, privacy issues do not only arise only from people that are using the service that is collecting data like in the traditional internet environment but also from people that do not use these smart devices (Atzori, Iera & Morabito, 2010).

The personal data harvesting operated by IoT devices leads to privacy concerns especially in the smart home context. The first concern is about concealing location information

[5] 10e-9 euro per byte in 2010

(Schurgot, Shinberg & Greenwald, 2015). For many smart devices, location is a crucial information to provide the expected service or an additional one (e.g. a smart thermostat adapting temperature to the outside weather as already mentioned in the “hardware security” part). Usually, the users must accept to disclose their location to the IoT server. This information, if leaked, could help a malicious individual determine the household’s routine and even determine if the user is at home or even on holidays abroad. A second concern, identified by Schurgot, Shinberg & Greenwald (2015), is what is called mobile presence spoofing. Many IoT devices have their own dedicated mobile application to display, inter alia, the status of the connected device, the data it has collected so far, … Even though the IoT device might not be collecting any location data, the mobile app could thanks to the phone’s integrated GPS.

Solutions to improve user’s privacy exist and are often referred to as PET (Privacy Enhancing Technologies).

3.4.3. INTEROPERABILITY

The last major challenge we decided to address in this work is that of the interoperability of objects. This challenge must be overcome in order for the IoT to deliver on its promises.

In the literature, an interested reader may find many definitions of interoperability. Among them, we have decided to present two of them, that we believe, fit well with the context of the IoT (Noura et al., 2019).

The first, and more general one, comes from IEEE website which defines interoperability as "The ability of two or more systems or components to exchange information and to use the information that has been exchanged". (IEEE Standard Computer Dictionary, 1990)

The second definition comes from ISO/IEC 2382-1:1993(en) which defines interoperability as "The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units".

3.4.3.1. Standardization/uniformization

The interconnectivity of objects is at the basis of the IoT paradigm and is even often considered as the backbone of the Internet of Things (Samuel, 2016). Nevertheless, it is currently impossible to assert that this intercompatibility of objects exists on a large scale for several reasons that we will review in this section.

When we talk about interconnectivity of connected objects, we are talking about one of the most disturbing problem affecting users of connected objects. In today's world, finding connected objects is one thing, but managing them is another. Indeed, a criticism often addressed by users towards these devices is their lack of uniformity and intercompatibility. Indeed, as we have already mentioned it previously, the IoT sector is booming and many brands are trying to establish themselves as leaders in this market by imposing their standard both in terms of hardware and communication protocol. This policy, conducted by many brands, prevents objects of different brands from cooperating/communicating, or in some cases, allow them to cooperate and communicate but only on a sub-optimal level with limited capabilities.

This has two main effects. The first one mainly benefits the brands selling connected objects. Indeed, this lack of compatibility with competitors makes the consumer dependent on the brand and its partners for any future purchase of connected objects. This lack of compatibility will indeed increase consumer loyalty by increasing the consumer’s switching costs. When the user will be wanting to add a new object to its network of connected objects, he will turn to this same brand to ensure, firstly, that it can be integrated into his current network and, secondly, to ensure that he can benefit from all the features of his new object to their full potential. Moreover, as Miori & Russo pointed out,

Many domotic systems crowding the market are rarely interoperable and thus do not permit consumers to choose devices according to their requirements or other relevant criteria, such as cost, performance, trends and confidence, instead of being constrained by issues of compatibility with their pre-existing systems. (Miori & Russo, 2014, p. 811)

The second effect, equally unpleasant for the user, is the multitude of connected object management applications that must be installed in order to manage the network of connected objects if they come from different brands. From Google Home to Google Nest to SmartThings or even Philips Hue, each brand offers its own connected device management

software which makes network management even more complex and time consuming for the user by flooding its PC, smartphone or tablet with many different apps.

As you will certainly have understood, when talking about intercompatibility, communication protocols is a cornerstone. As Miori and Russo (2014) pointed out during the 28th Conference on Advanced Information Networking and Applications Workshops, "no domotic tech has emerged as a de facto standard in the industry" and numerous connectivity protocols currently exist all having their inherent advantages and drawbacks. We believe that it is important to take a quick look at the most prevalent ones as one of them could establish itself as a standard in the market in the coming years.

1) Wi-Fi HaLow (IEEE 802.11ah)

As defined by Cisco, “Wi-Fi is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smartphones and wearables), and other equipment (printers and video cameras) to interface with the Internet. It allows these devices to exchange information with one another, creating a network.” (Cisco, 2020).

Wifi is based on the IEEE 802.11 standard which “defines the protocols that enable communications with current Wi-Fi-enabled wireless devices, including wireless routers and wireless access points.” (Cisco, 2020). Wi-fi has some features that differentiate it from other standards. Firstly, the huge data rate it can provide (1Gbps). Secondly, it also provides an important nominal range that can go up to 150 meters. A third unique characteristic of Wi-Fi is that it is a trademark of the Wi-Fi Alliance. This means that it can only be used on products that have passed a test known as the "Wi-fi Alliance certification test" where, among other things, the compatibility, performance and conformity of the product are tested. This certification test ensures the customer that every equipment is compatible with other Wi-Fi certified object (Samuel, 2016 & Wi-Fi Alliance, 2020).

Nevertheless, this technology might not fit the needs of IoT for several reasons. First of all, the important data rate provided might require too much power for many IoT applications and battery-operated devices. Secondly, the IEEE 802.11 standard is only effective at the nearest access point which prevents it from being used in large homes or without the need of signal repeaters (Samuel, 2016). Thirdly, a side effect of being a trademark of the nonprofit Wi-Fi alliance is that Wi-Fi is thus not an open source standard. To obtain the Wi-Fi

certification, companies have to pay an annual fee and need to pass the certification test which can limit the number of companies and number of products using that standard ("Membership | Wi-Fi Alliance", 2020).

In 2017, to counterbalance the above-mentioned flaws, the Wi-Fi alliance published IEEE 802.11ah, a new wireless networking protocol also referred to as Wi-Fi HaLow ("Wi-Fi HaLow | Wi-Fi Alliance", 2020). This protocol has specially been designed to support the concept of IoT by extending the range of Wi-Fi networks by using a lower frequency band (900Mhz compared to 2.4 GHz and 5 GHz bands for conventional Wi-Fi networks), lowering the energy consumption and allowing the creation of large groups of sensors that cooperate to share signals (Qualcomm Technologies, Inc., 2016).

2) Bluetooth LE (also known as Bluetooth Smart)

Bluetooth LE (IEEE 802.15.1) is an open standard based on the Bluetooth technology developed by Nokia back in 2006. Bluetooth Smart was also born as a result of the importance of the IoT wave.

Compared to the traditional Bluetooth standard, Bluetooth Smart allows a data rate of the same magnitude (1 Mbit/s) for a power consumption 10 times smaller. Thanks to this lower power consumption, this technology can be integrated into new types of equipment such as IoT devices at a very cheap cost. Unlike conventional Bluetooth, the range of BLE is way smaller with a 10 meters nominal range.

The traditional Bluetooth and Bluetooth LE are meant to be complementary as they serve different purposes. As explained by Link-Labs on their website:

Bluetooth can handle a lot of data but consumes battery life quickly and costs a lot more. BLE is used for applications that do not need to exchange large amounts of data and can therefore run on battery power for years at a cheaper cost. It all depends on what you’re trying to accomplish. (Ray, 2015)

3) ZigBee

Unlike the two previous protocols and being based on the IEEE 802.15.4-2011 standard, Zigbee is not an evolution of an already existing protocol but was created to meet the specific needs of wireless personal area networks (WPAN) and uses radio waves. Characterized by very low costs of production and low consumption, Zigbee tries to impose itself as the reference in home automation for small objects such as smart sensors with a range from 75 to 100m indoors and 300 meters outdoor (line of sight) ("Zigbee - Zigbee Alliance", 2020). Zigbee is an open-source network, the compatibility between all Zigbee enabled devices cannot be always guaranteed (50five.be, 2020).

4) Z-Wave

Just like ZigBee, Z-Wave was created to meet the needs of the IoT and more specifically home automation. Also using radio waves as communication channel, Z-Wave is, unlike its direct competitor, not open source and is being managed by the American company Sigma Designs following the acquisition of the Danish firm Zen-Sys in 2008 (50five.be, 2020). Manufacturers using this technology are grouped together within the Z-wave alliance, which ensures the compatibility of the products produced within the alliance (Z-Wave Alliance, 2012). Other notable differences between these 2 competitors are the frequency band they use, the number of connectable objects per network they propose and the range of communication (Samuel, 2016). The frequency range used by Z-wave is just under the Gigahertz milestone which also constitutes an important advantage. Because of that, objects using the Z-wave protocol do not communicate at the same frequency band as other traditional Wi-Fi or Bluetooth devices within the home environment, and are thus avoiding interferences and stability problems that technologies such as Zigbee may encounter due its 2,4 Ghz frequency band (50five.be, 2020).

	Wi-Fi	Bluetooth LE	Zigbee	Z-Wave
IEEE standard	802.11	802.15.1	802.15.4	802.15.4
Frequency band	2.4 GHz, 5 GHz	2.4 GHz	2.4 GHZ	900 MHz
Nominal range	150 m	10 m	100 m	30 m
Peak current consumption	116 mA	12.5 mA	30 mA	17 mA
Power consumption per bit	0.00525 µW/bit	0.153 µW/bit	185.9 µW/bit	0.71 µW/bit
Data rate	1 Gbps	1 Mbps	1Gbps	100 Kbps
Number of nodes per network	250/Access point	One-to-many	65000	232

Table 4 - Characteristics of home network wireless standard based on Samuel (2016).

When looking at these main standards, we quickly notice that there are two different major types of wireless protocols used in home automation. First of all, the more known and already widely spread wireless standard used for other purposes than the ones of connected objects and home automation. On the other hand, other standards are emerging to meet the specific needs of the IoT and are born due to the inherent challenges brought by the IoT. Each standard currently used has a clear advantage over the others, but no standard has yet been established as a clear leader on the market. This lack of leadership creates a disparate market

in which objects that could have cooperated if they were operating under the same standard do not cooperate due to lack of standardization. The emergence of a common framework between all manufacturers in the home automation field, allowing all smart devices to be fully interoperable would bring tremendous added value to the customers.

3.5. POTENTIAL SOLUTIONS TO IOT CHALLENGES

In this section, we will explore the different solutions provided by the literature to the different challenges that we previously outlined in section 3.6. The aim is mainly to get an overview of the techniques currently being developed to overcome these different and complex challenges.

3.5.1. SECURITY

As mentioned above, hardware is too often not protected by the manufacturer. In the smart home context, hardware vulnerabilities may seem more complex to exploit because the potentially vulnerable objects are located in a relatively hard to access environment, i.e. the home. Nevertheless, these hardware-level vulnerabilities can still be remotely exploited. In order to ensure the object's integrity, a first advice found in the literature is to block access from a UART console. The hacking of a smart device is often successful when hackers have an unrestricted access to a UART console which they use to change the boot parameters of the unit and extract the login information.

A second tip, widely discussed in the literature, is the use of better hashing algorithms that increase the password entropy[6] and makes it less trivial to brute force. As already stated before, the hashing algorithms used for connected objects are often the same as those we can encounter on our PCs and do not take into account the inherent characteristics of connected devices. In recent years, several works have been carried out with the aim of developing smart objects specific algorithms, which would allow to ensure a satisfying level of security while taking into account, among other things, the low computing capabilities and

[6] The entropy is the level of unpredictability of a password.

autonomy of the connected objects. An IoT specific design-for-security methodology is still very needed.

A third technique that can be implemented is to secure the update channels. Indeed, updates of connected objects are a headache for the manufacturers. Forcing users to return to their point of sale to update their product is not a feasible method in the long term and remote updates are complex for objects with such limited resources. Nevertheless, updates are necessary in order to be able to patch any existing flaws that, if exploited, could harm the integrity of the smart object and the home network in general.

Finally, several elements such as the filesystem[7] and communication channels need to be encrypted to make it harder for an ill-intentioned individual to modify them. In order to encrypt communication channels, the TLS (Transport Layer Security) cryptographic protocol can be used by the manufacturer to "provides end-to-end security of data sent between applications over the Internet" ensuring that private data such as passwords, personal correspondences, … cannot be retrieved by eavesdroppers and hackers ("What is TLS & How Does it Work?", 2020). That leads us to the following point about ensuring privacy.

3.5.2. PRIVACY

The challenge of privacy is, for the most part, already widely known by companies in view of the scandals that have arisen in recent years. Now, it is not uncommon to see companies taking PIAs (Privacy Impact Assessments) to determine the impact of their product on the privacy of each and every stakeholder involved in the process. These PIAs were introduced with the General Data Protection Regulation (GDPR Art. 35) and have had an unprecedented impact on the vision of privacy in a digital context ("Privacy Impact Assessment", 2018). In addition, some techniques aimed at preserving the privacy of individuals on the Internet can be used in the context of connected objects. These technologies are often referred to as PETs (Privacy Enhancing technologies) or PPTs (Privacy Preserving Techniques).

[7] A *filesystem* is the methods and data structures that an operating system uses to keep track of files on a disk or partition; that is, the way the files are organized on the disk. (The Linux Documentation Project) https://www.tldp.org/LDP/sag/html/filesystems.html

Indeed, a solution that is booming today and abundantly discussed in the literature is the use of a VPN (Virtual Private Network) to cover the true geographical location of objects. Indeed, location details of smart objects are revealed by a user's IP address a solution to hide their location is to set up a VPN server to proxy communication between a user's home network and the cloud where the data is often stored. As smart objects are often linked to a mobile application for remote controlling, the phone can also reveal details about the user's location. A solution is to use a fake GPS location app to hide the user's exact location.

3.5.3. STANDARDIZATION/UNIFORMIZATION

This is the challenge over which a company has the least amount of decision-making power. As mentioned earlier, there is currently no de facto standard in the IoT environment. As a result, the IOT promise is not yet fully fulfilled as full intercompatibility is still not reached. Certainly, some solutions such as IFTTT (If This Then That) already allow thousands of objects and applications to communicate and form scenarios (e.g. communication between weather sensors and lights: lower the shutters when it starts raining), but the possibilities are still limited due to the different protocols used by the multiple actors on the market. The emergence of a common communication standard for all connected objects is necessary to achieve the goal of the IoT. It is therefore important for companies to follow with interest the advances of Standard Development Organizations (SDOs) in order to adopt the protocol that will later become the industry standard. These organizations aim at building standard platforms, protocols, and technologies to ensure seamless operation of these devices.

Challenges	Solutions	Implications
Security	Securing hardware level vulnerabilities	Blocking/restricting the access to the UART console and to the smart objects' components in general
	Better securing of the root password of the device thanks to IoT-specific hashing algorithms	Staying on the lookout for new hashing algorithms developed specifically for IoT security
	Using secure update channels and making regular software updates on the long term	Developing a sustainable update plan capable of patching remotely discovered vulnerabilities Not using the same default password for a product and making sure customers modify their password as soon as they connect it to their private network Adopting a PUSH strategy rather than a PULL one for updates
	Multiple elements encryption	Encrypting elements such as the filesystem and the communication channels thanks to well recognized security protocols (i.e. TLS for communication channels)
	Adopting a security-centric approach from the design of the connected object itself	Choosing the right development strategy (i.e. developing a competitive advantage thanks to short TTM or developing a long-lasting competitive advantage by granting users secure products)

Privacy	Taking Privacy Impact Assessments	Making a complete analysis of the impact of the object developed on the privacy of all the involved stakeholders
	Adopting Privacy Enhancing technologies and Privacy Preserving Techniques	For the customer, using a VPN is a way of covering its true geographical location and ensuring a higher level of privacy than the one the object is already proposing. Ensuring privacy also includes the management of the data transmitted by the connected objects management apps. For companies, the first implication is of course acting according to the local regulation in terms of data collection. Moreover, no matter the local regulation, ensuring that both the connected object and its management app are collecting only meaningful data to ensure the proper functioning of the device and potential enhancements is of course key to gain customers trust.
Standardization/uniformization	Solution yet to be developed	Paying close attention to or actively participate in the design of a common communication standard for IoT smart home devices and appliances.

Table 5 - Summary of the main challenges, potential solutions and their implications.

3.6. REQUIREMENTS AND MANAGERIAL IMPLICATIONS

Another important theme of this work concerns the implications related to the development of an IoT-enabled smart home. The main implications identified in the literature are identified in this part for the purpose of helping businesses better develop their solutions and implement their products in the users' households.

First, there is a need to develop some core competencies. In that sense, businesses require skills in: product development and marketing, wireless communication, and data management (Saarikko, Westergren & Blomquist, 2017; Lee and Lee, 2015). In fact, the IoT offers the possibility to gather data on product usage. That feedback can then be used for product development and marketing purposes such as prioritizing certain features over others or better solve (potential) issues with the product, for instance. Technical knowledge on wireless communication is also a critical skill as it allows to develop solutions and solve problems related to interoperability and interconnection of 'things', which is a key asset for the enhancement of home automation. Strong capabilities in data management are also required as value is created from the analysis of vast amounts of data. This involves expertise in data aggregation, filtering, analysis, and finding correlations in data generated from a large number of users (Lee & Lee, 2015). Big data and data analytics skills are therefore crucial. As the three aforementioned fields are critical, a competitive advantage could be derived from very strong expertise in those fields.

In addition, other more specific skills in the technologies making part of the IoT framework (e.g. middleware, cloud computing) are also important but might not be as crucial as the ones mentioned earlier (Lee & Lee, 2015).

Second, it is important for managers to decide which competencies will be internalized in the company and which ones will be externalized. While internalizing competencies allows for more control it can be costly and time consuming to build up expertise from scratch. Externalizing some of the competencies can allow to free up more time and resources for the internalized competencies while still achieving top performance by leveraging the recognized expertise of external partners. Externalizing also increases dependence on other companies

and therefore it is important to decide on which competencies can and should be externalized.

Third, developing partnerships is key. As stated before, some of the competencies should be externalized and finding the right partners then becomes a key asset. Here, information sharing, and collaboration are crucial and involve multiple parties and perspectives. Access to those external competencies can be fostered by value networks, ecosystems, or partnerships (Lee & Lee, 2015; Saarikko, Westergren & Blomquist, 2017).

Fourth, companies need to be ready to adapt their business models. To that regard, several main implications can be considered: solution-based versus product-based value propositions, horizontal versus vertical diffusion, and industry changes. Solution-based value propositions are based on solutions rather than products. For instance, a user will not purchase an appliance but instead pay a monthly fee for carefree use of the appliance. This ensures that the user is not subject to problems linked to the appliance such as technical issues or obsolescence. This would also allow the company to have a more predictable fixed monthly expense and revenue as well as forcing it to have ongoing contracts, encouraging more stable relationships with customers. In term, this raises barriers to entry for competitors (Saarikko, Westergren & Blomquist, 2017).

Connected products require a broad skill set (broader than for non-connected products) and therefore several parties, with their respective expertise, might work together towards a co-created solution (Burkitt, 2014). Although they are working towards a common goal, each actor also has his own business interest. In that sense, two contradictory business logics exist: vertical diffusion and horizontal diffusion.

With horizontal diffusion, an actor will try to leverage his expertise (usually knowledge of a particular technology) to as many customers as possible, regardless of industry or market. In contrast, an actor pursuing a vertical diffusion strategy will aim to stay in the same industry in order to establish a firmer presence (Saarikko, Westergren & Blomquist, 2017). These contradictions in business logics might create difficulties when partners pursuing opposite logics need to cooperate. Hence, when managers negotiate mutually beneficial agreements with partners, they should take into consideration the business logic pursued by their partners.

Fifth, managers need to know what they will do with the data and insights they have gathered. While they will of course use the insights for their own purposes, customers will also be interested in the data collected. Two options are considered: sharing or selling. In case the company decides to share the information on a free basis with the customer the perceived quality of the product will be increased without any additional cost. In the case of a sale, the company will propose additional services derived from the data collected on product usage, for an extra fee. A link can be made with servitization (Saarikko, Westergren & Blomquist, 2017; Oliva & Kallenberg, 2003).

Sixth, the **data collected should be used to refine different parts of the value chain**. A lot of valuable data can be gathered such as location, status, and usage. Saarikko, Westergren & Blomquist (2017) highlight that data can then be used to enhance several elements of the value chain such as efficiency in the supply chain, better service and maintenance, and improved product development. In addition, customer behavior can be better analyzed, and more personalized offers can then be proposed.

From a supplier perspective, valuable information can be collected concerning product wear and tear, product usage, relative importance of different features of the product, and more (Saarikko, Westergren & Blomquist, 2017). This information can be used as input to improve existing products (incremental innovation) and/or encourage future development (disruptive innovation), based on hard data. Indeed, in the past, product developments did not have access to as much data as it is now possible and therefore, past improvements relied more on intuition and past experience. Also, a key aspect in product development is to understand which product or service features are critical to the customer and which ones can be omitted. The data that is now possible to collect opens up opportunities to enhance feature prioritization, leading to increased revenues and lower production costs.

From a marketing perspective, product-based services can be proposed, which allows to provide added value to customers in comparison to traditional products. With connected products, companies can operate based on real-time data and proactive service, which allows them to propose a dynamic product and service environment with regular software updates and where some actions (e.g. maintenance) can be carried out when they are actually needed,

instead of on guessed time intervals (e.g. every 6 months) (Saarikko, Westergren & Blomquist, 2017).

Seventh, managers need to understand what aspects of home automation are the most appealing to users. We have mentioned earlier that it was important to understand what features of a product matter (the most) to customers. Here, the focus lies more on the reason why customers need automation, not necessarily on the product features themselves. In their study, Brush et al. (2011) identified convenience (including laziness), peace of mind, security, and centralized control as the users' favorite aspects of home automation. Depending on each product's purpose, preferences might be different.

Eight, data ownership should be a core concern for managers. The data is generated by the user's actions but is collected, stored, processed, analyzed, and presented by the product's manufacturer and eventually other third parties. In addition, some data are considered personal or even sensitive and different industries and markets have their own rules. Also, local regulations need to co-exist with regional regulations. All of this leads to a plethora of rules and considerations regarding data ownership. It is crucial for managers to know what can and cannot be done with the collected data in each specific situation. We will come back to the privacy challenge and the tools available to users to protect themselves in this work.

Ninth, it is very important to adopt a user-centric perspective when developing the product. An IoT-enabled smart home is a complex system that incorporates various technologies. A lot of efforts are therefore put on the technical development of the system. It then becomes easy to be submerged by the technical perspective and (unintentionally) neglect the user-centric perspective. However, the end goal is to deliver value to the home's occupants and therefore adopting a user-centric view is essential. Centering the system on the user will allow to increase user acceptance (Reinisch et al., 2011).

Tenth, the user should be empowered when using the system and the system should have some degree of adaptability. Barriers to user adoption of a smart home include a lack of appropriation of the system and its functions. Some end-users might be uneasy with the implementation of new technologies in their homes as well as unsure in their ability to manage them. For these reasons, end-users should be provided a simple, confidence-building system with some degree of personalization (Brush et al., 2011). Although the system is

complex from a technical point of view, it should be easy for end-users to manipulate and customize the different functions of the system. This is especially the case for solutions that aim to improve daily lives of elderly. More briefly, the system should be able to adapt to the end-user, not the opposite.

Eleventh, focus on comfort creation when developing an IoT-enabled smart home solution. Reinisch et al. (2011) have found out, through their ThinkHome project, that comfort was one the main criterions for customers to acquire expensive home automation technology. Besides comfort, energy was also an important feature for customers as it is linked with sustainability and economic considerations.

Twelfth, the home automation system should follow a modular architecture. The system should allow to easily integrate intelligent control strategies, interface with additional (external) services, and flexible extension and exchange of existing or new components. In other words, elements such as components or services should be added or removed from the system with relative ease. Reinisch et al. (2011) denote that the design should be an open system, operating on open standards, open software, and provide open interfaces to other systems and domains. The system should also transparently integrate different parts (i.e. devices, protocols, parameters, data).

Thirteenth, sustainable IoT based home automation solutions should be flexible and scalable. IoT systems need to manage hundreds to thousands connected devices. The systems need to be able to accommodate an increasing number of devices, as households tend to accumulate devices over time.

Indeed, as systems are expensive, technology embedded into the devices evolves as well as user needs it should be accounted for that systems will evolve, hence need to accommodate changes and new devices with ease. If the systems have poor scalability, the workload will increase by the same factor the number of connected devices scales up, which is contrary to the principles of an efficient and sustainable solution. Besides scalability, systems also need to be flexible as they will need to adapt to the different occupants of the households (Saarikko, Westergren & Blomquist, 2017).

Fourteenth, building an efficient and effective data mining process starts at the device's (local) level. Large amounts of data are being collected by the system, that then need to be filtered out. In order to decrease the amount of data filtered at a central level (back office system), the devices should start filtering the data themselves and forward only relevant data with their respective back office system (Saarikko, Westergren & Blomquist, 2017).

CHAPTER IV - SMART HOME USER ADOPTION

In this work we try to identify the main managerial implications that foster the development of the smart home market. In that sense, determining the barriers and enablers to market adoption of smart homes allows us to identify their related managerial implications. In order to better understand the market needs and identify the main barriers to adoption of the technology, it appears relevant to investigate both user-centric (market-pull models) and technological developments (technology-push models). Since technological developments have already been mentioned earlier, this section will shed a light on the user needs. More specifically, this section will review the literature related to user adoption of IoT-enabled smart homes.

Several previous studies have attempted to model user adoption of smart home services. In most cases, inspiration is drawn from very general models and were adapted by adding and/or removing context-specific variables. Hence, most models are developed with a top-down approach, where general variables are identified first, and more context-specific variables are added to the model afterwards to better match with the specific context of adoption. For this reason, we reviewed the Technology Acceptance Model (TAM). Since this model is very general and not specific to the smart home context, we present the main findings done on this model and include a more elaborated review of the TAM in the Appendix 7 of this work. Then, the smart home specific models will also be reviewed in this part. The smart home specific determinants used in previous works are combined in order to a more coherent whole.

4.1. General Adoption Model: Technology Acceptance Model (TAM)

4.1.1. TAM

An often-mentioned model to study user adoption of a technology is the Technology Acceptance Model (TAM). It was first developed in Davis (1989). The TAM analyses two key beliefs: perceived usefulness and perceived ease of use, and users' attitudes, intentions and actual computer adoption behavior (Davis, Bagozzi & Warshaw, 1989). Perceived ease of use corresponds to "the degree to which a person believes that using a particular system would be free of effort" and perceived usefulness to "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989). In addition, Davis (1989) states that the perceived usefulness of a system is influenced by its ease of use because the easier it is to use a system, the less effort it requires, and the more useful it becomes. Also, Davis, Bagozzi and Warshaw (1989) state that "all else being equal, people form intentions to perform behaviors toward which they have positive affect", which highlights the link between attitudes (the general impression of the technology) and behavioral intentions.

The TAM has been studied a lot and more elaborated versions have emerged. The most notable improvements are the TAM 2 (Venkatesh & Davis, 2000; Venkatesh, 2000), the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003), and the TAM 3 (Venkatesh & Bala, 2008).

4.1.2. TAM 3

The TAM 3 combines the determinants of perceived ease of use and perceived usefulness identified in previous works. More specifically, Venkatesh and Davis (2000) empirically validated the general determinants of perceived usefulness: subjective norm, image, job relevance, output quality, result demonstrability, and perceived ease of use, as well as two moderating variables (i.e. voluntariness and experience). In parallel, Venkatesh (2000) stated that system users form early perceptions of perceived ease of use based on several anchors related to their own general beliefs regarding computers and computer use. The anchors identified by Venkatesh (2000) of perceived ease of use are: computer self-efficacy, perception of external control, computer anxiety, computer playfulness, perceived enjoyment, and objective usability. In the TAM 3, Venkatesh and Bala (2008) provide empirical

evidence that experience affects determinants of perceived ease of use (i.e. computer anxiety, computer playfulness, perceived enjoyment, objective usability). In the following table we propose an overview of the determinants identified in previous works:

Perceived usefulness determinants, as identified in (Venkatesh & Davis, 2000)	Perceived ease of use	The degree to which a person believes that using an IT will be free of effort (Davis et al., 1989).
	Subjective norm	The degree to which an individual perceives that most people who are important to him think he should or should not use the system (Fishbein & Ajzen, 1975; Venkatesh & Davis, 2000).
	Image	The degree to which an individual perceives that use of an innovation will enhance his or her status in his or her social system (Moore & Benbasat, 1991).
	Job relevance	The degree to which an individual believes that the target system is applicable to his or her job (Venkatesh & Davis, 2000).
	Output quality	The degree to which an individual believes that the system performs his or her job tasks well (Venkatesh & Davis, 2000).
	Result demonstrability	The degree to which an individual believes that the results of using a system are tangible, observable, and communicable (Moore & Benbasat, 1991).
Perceived ease of use determinants, as identified in (Venkatesh, 2000)	Computer Self-Efficacy	The degree to which an individual believes that he or she has the ability to perform a specific task/job using the computer (Compeau & Higgins, 1995a, 1995b).
	Perception of External Control	The degree to which an individual believes that organizational and technical resources exist to support the use of the system (Venkatesh et al., 2003).
	Computer Anxiety	The degree of "an individual's apprehension, or even fear, when she/he is faced with the possibility of using computers" (Venkatesh, 2000, p. 349).
	Computer Playfulness	". . .the degree of cognitive spontaneity in microcomputer interactions" (Webster & Martocchio, 1992, p. 204).
	Perceived Enjoyment	The extent to which "the activity of using a specific system is perceived to be enjoyable in its own right, aside from any performance consequences resulting from system use" (Venkatesh, 2000, p. 351).
	Objective Usability	A "comparison of systems based on the actual level (rather than perceptions) of effort required to completing specific tasks" (Venkatesh, 2000, pp. 350–351).

Table 6 - determinants of perceived usefulness and perceived ease of use.

An overview of the TAM is provided in the following figure:

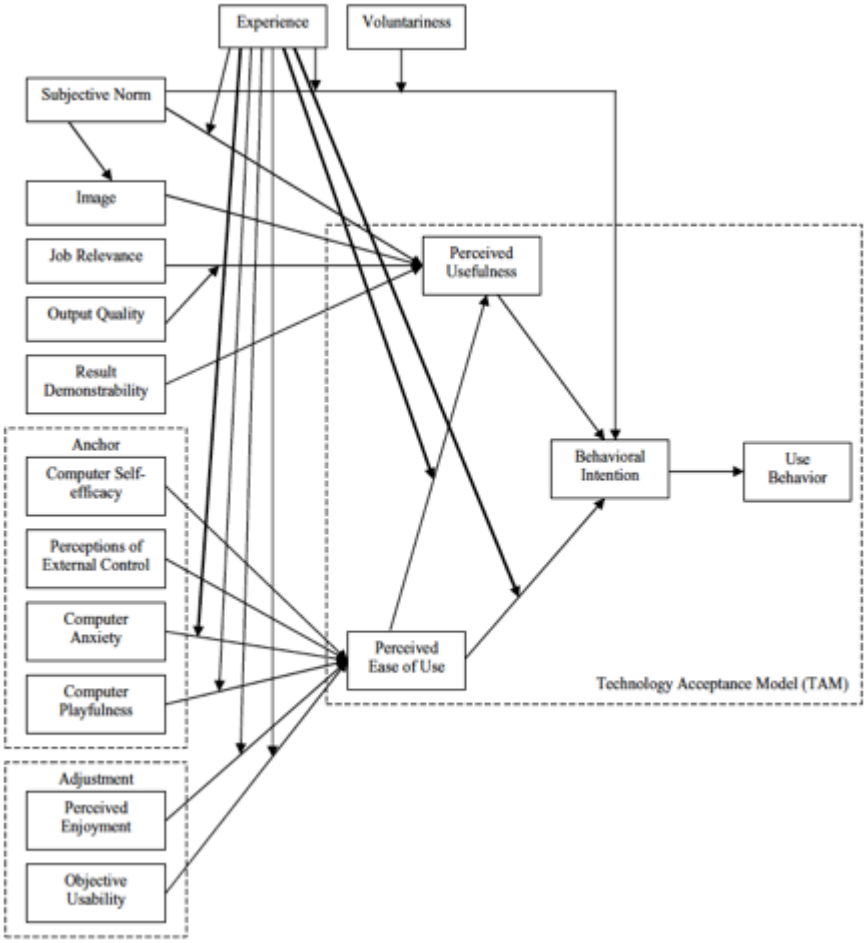


Fig. 5 - TAM 3 as presented in Venkatesh & Bala (2008).

Further, the TAM 3 was also aimed at providing interventions that managers could undertake at pre- and post-implementations stages of new IT systems inside the company, in order to influence the determinants of perceived usefulness and perceived ease of use. As these interventions are focused on the implementation of a new system in the organization context, we do not find it sufficiently relevant to be included in this part. However, we suggest the interested readers to consult the more elaborate review on the TAM in the Appendices part of this work.

4.2. SMART HOME CONTEXT-SPECIFIC MODELS

Besides the generalist models that have been developed, other more context-specific models have also emerged. These more specific models usually draw inspiration from the generalist models and are adapted to a specific domain by adding and removing context-

specific variables. The context that is of interest to us is of course the smart home context. Hence, in this part we review the main advances observed in IoT-based smart home adoption models.

We first review the main models that have been adapted to the smart home application. Then, we review some interesting results that have been achieved in the literature. We also list the main determinants that have been used in past research.

4.2.1. MODELS

Park et al. (2017) use a smart home adapted TAM as research model (i.e. original TAM version 1 with five external factors) and investigate the collected data using a structural equation modelling (SEM) method and conduct a confirmatory factor analysis (CFA).

Shin, Park and Lee (2018) propose two different studies. A first study is aimed at adapting the TAM to the smart home context in order to infer the consumers' intentions to adopt smart home services. Two external factors – compatibility and privacy – are added to the original TAM to explain attitude. Moderator variables such as age, gender, income level and education level were also used. The second study in (Shin, Park and Lee, 2018) is based on a *multivariate probit model* and aims to describe the diffusion (i.e. adoption rate) of smart homes. Shin, Park and Lee (2018) use gender, age, education level, monthly average income, number of household members, type of housing, amount of ICT devices and home appliances possessed, level of recognition and usability of smart home appliances, level of usability of smart home appliances, and importance of personal information protection to explain the consumers' intention to purchase within a specific timeframe (i.e. 6 months, 1 year, 2 years, 3 years, more than 3 years). The insights drawn from the second study in (Shin, Park & Lee, 2018) allow to make a parallel with the famous works of Rogers on innovation diffusion (Rogers, 2010). Kim et al. (2016) studied the willingness to pay for smart home services of consumers, using a contingent valuation method.

Kim, Park and Choi (2017) take a different approach to study adoption of IoT-enabled smart home services. In opposition to what other research models do (e.g. Park et al., 2017; Shin, Park & Lee, 2018), they propose a new type of model combining the Technology Acceptance Model (TAM) with a Value-Based Adoption Model (VAM). While the TAM is a very commonly

used model, it also has some drawbacks and therefore Kim, Park and Choi (2017) combine it with a VAM to mitigate these effects and propose a research model they claim is more suited to the IoT-based smart home application. More specifically, the user characteristics and environment studied in the TAM are not appropriate to study user adoption of smart home as users should be considered as consumers and there is a substantial difference between the organizational environment and private sphere, where usage is encouraged by the individual himself instead of the organization. The importance to take into consideration such social aspects (e.g. user characteristics and environment) in order to better understand smart home adoption was also expressed in (Ginter, 2001) and (Yang, Lee & Lee, 2018). Kim, Park and Choi (2017) identify privacy risk, innovation resistance, technicality and perceived fee as determinants of perceived sacrifice, whereas perceived benefit is influenced by facilitating conditions, usefulness, and enjoyment. Perceived value is influenced by perceived sacrifices and benefits and influences both attitude and intention to use.

4.2.2. RESULTS

Park et al. (2017) provide empirical evidence that compatibility, connectedness, and control have a positive effect on user acceptance of a smart home whereas cost has a negative impact. Enjoyment was ruled out of the model as it was non-significant. Park et al. (2017) were able to predict 95% (R2=0,95) of the variance of perceived usefulness with perceived compatibility, perceived connectedness, and perceived ease of use as determinants. Surprisingly, perceived ease of use appeared to be a better predictor of attitude than perceived usefulness, which is in contradiction to what is usually the case in the TAM.

Gao and Bai (2014) validate social influence, perceived control, enjoyment, as well as the original factors of the TAM – perceived ease of use and perceived usefulness—as the main determinants of user intentions regarding IoT technologies.

In the smart home-adapted TAM of Shin, Park and Lee (2018), compatibility, perceived ease of use, and perceived usefulness are significant determinants of purchase intention. This is consistent with what was observed in (Park et al., 2017).

The “multivariate probit model” of Shin, Park and Lee (2018) indicates that older consumers are more likely to purchase smart homes within a given time period than are younger consumers. From (Shin, Park & Lee, 2018) it can be learned that the proportion of respondents that want to purchase smart home services within one year is much smaller than those who plan to purchase in more than one year. Unsurprisingly, Shin, Park and Lee (2018) find that higher income levels lead to faster purchase of smart home appliances but have no significant influence on purchase intention. On the contrary, it is found that education level, family size and housing type do not significantly influence adoption time of smart homes. Overall, older people with higher income level tend to purchase smart home appliances faster than younger people (Shin, Park & Lee, 2018). Another interesting finding in (Shin, Park & Lee, 2018) is that respondents who believe that smart homes are useful tend to purchase smart home appliances within less than two years. This is consistent with their other study that highlights perceived usefulness as a statistically significant factor of attitude and use intention. From a marketing perspective, Shin, Park and Lee (2018) find that early recognition (awareness) of smart home appliances does not make consumer purchase faster, except for safety and security products. Hence, early recognition is expected to have little impact on the initial diffusion of the smart home market.

Yang, Lee and Lee (2018) consider automation, remote controllability, interconnectedness, and reliability as crucial factors for smart home service acceptance. Their model was able to explain 47,9% of the variance of adoption intention. Automation was not statistically significant. Yang, Lee and Lee (2018) suggest high device prices, limited consumer demand, long device replacement cycles as reasons for the still limited diffusion of the smart home market. Moreover, Ricquebourg et al. (2006) suggest the lack of technology to establish the infrastructure of a smart home as the largest barrier of its mainstream adoption. To that regard, Park et al. (2017) foresee that smart home acceptance with IoT technologies will expand as access to wireless networks and compatibility between operating systems, languages, and frameworks will develop.

Edwards and Ginter (2001), on their side, suggest that social aspects such as user characteristics and environment have been overlooked in smart home adoption and diffusion research. Yang, Lee and Lee (2018) also highlight the need to consider user characteristics and

environment in smart home acceptance studies as results were different across different groups.

4.2.3. DETERMINANTS

The determinants that have been used in the literature to study smart home adoption are the following ones.

- **Innovation resistance**

Kim, Park and Choi (2017), as well as Choi (2015), suggest that innovation resistance will be high for smart home adoption. In (Kim, Park & Choi, 2017), innovation resistance is defined as "a negative attitude regarding changes brought on by adoption of smart home service" (Ram, 1987; Oreg, 2006), and is classified amongst the significant determinants of perceived sacrifice.

- **Perceived connectedness**

Park et al. (2017) suggest that the ability to use and control the home network (and appliances) wirelessly leads to a sense of feeling of convenience. This idea is gathered under the term 'perceived connectedness'. Perceived connectedness contributes to both perceived ease of use and perceived usefulness. In (Yang, Lee & Lee, 2018) the term 'interconnectedness' is used and refers to the ability to connect devices, applications and services with each other and make them work together. It is expected from a smart home that devices have the ability to adapt to changes in preferences, requirements, and needs of a user (Edwards & Grinter, 2001). Conceptually, new devices should be integrated to the system easily. However, it is not the case in reality and interoperability is therefore one of the main barriers to adoption of smart homes (Balta-Ozkan, 2013).

- **Perceived Compatibility**

In Rogers (2010) compatibility is defined as "the degree to which an innovation is well-operated in harmony with the traditional and present needs." Compatibility is presented in (Tsai, Chien, & Thai, 2014) as an important determinant of perceived usability of a particular system. Compatibility allows to minimize the switching costs and efforts required by traditional systems or services. Therefore, compatibility is expected to be a key aspect in IoT-

enabled smart homes (Asimakopoulos & Asimakopoulos, 2014). Park et al. (2017) confirm that intuition by highlighting perceived compatibility as a very strong predictor of perceived usefulness, and also identify an effect on perceived ease of use. Shin, Park and Lee (2018) and Bao et al. (2014) also find compatibility to be a significant determinant of smart home services adoption. They consider compatibility to be a critical factor as it allows to assess "how smart home services are interoperable with various home appliances and external services" (Shin, Park & Lee, 2018). In addition, compatibility is found to have more influence on attitude for women than men (Shin, Park & Lee, 2018).

- **Perceived control**

Park et al. (2014) define perceived control as "*the users' sense of how skillful it is to perform a particular activity using IoT technologies in smart home environments".* Demiris et al. (2008) identified perceived behavioral control as a determinant of perceived needs of consumers un using smart home sensor technologies. Park et al. (2017) suggest that a useful user interface that allows users to maximize user control skills should foster the perceived ease of use. Venkatesh et al. (2003) take perception of external control as determinant of perceived ease of use and define it as "The degree to which an individual believes that organizational and technical resources exist to support the use of the system."

- **Remote controllability**

In (Ji et al., 2016) and (Yang, Lee & Lee, 2018) controllability appears to be a significant factor in smart home adoption. Liu, Slotine and Barabasi (2011) argue that control is a critical issue in most complex systems. Remote controllability with mobile devices is a key factor as users prefer to control smart home services anytime and anywhere (Yang, Lee & Lee, 2018). Those devices become important to control the system; hence their user interface becomes key (Roduner et al., 2007). Kim, Park and Choi (2017) go further by underlining the need to develop a comprehensive user interface that can be used by older age groups, in order to positively influence the perceived technicality and attract that segment of people. Kim, Park and Choi (2017) consider non-monetary costs through the variable 'technicality', defined as the "degree of difficulty in using the relevant service process (non-monetary cost)". Yang, Lee and Lee (2018) also note that a network connection is essential when designing the smart

home. Hence, it should be considered as prerequisite to smart home adoption. Controllability refers to the ability to do whatever a user needs with the system (Kalman, 1959).

- **Perceived monetary costs (or 'perceived fee')**

In (Shin, 2009) perceived cost is considered as *"the concerns on the costs in buying, installing, maintaining and operating IoT technologies in smart home environments"*. Economic burden is identified in (Kim, 2008) and (Kim & Ammeter, 2014) as one of the highest barriers to adoption of new and innovative services. William, Bernold and Lu (2007) highlighted the key role of perceived cost of IT in users' intention to use. Park et al. (2017) highlight that perceived cost has a direct negative effect on user intention to use smart home services. In Kim, Park and Choi (2017) perceived fee is a monetary cost that influences perceived sacrifice and is defined as the "degree of users' perception regarding fee of smart home service (monetary cost)".

- **Perceived value**

Perceived value is defined as the "overall evaluation of the user regarding the benefit and cost of using smart home service" (Kim et al., 2007; Kim, Park & Choi, 2017). Park et al. (2017) suggest that users will deeply consider adopting smart home services if the benefits are worth the investment. Kim, Park and Choi (2017) show that perceived sacrifice and perceived benefits are significant determinants of perceived value. Perceived benefits' influence on perceived value is found to be much more important than the effect of perceived sacrifice on perceived value. Perceived value is found in several studies to have a high impact on attitude and intention to use (Kim, Park & Choi, 2017; Wang & Wang, 2010; Kim, Sun & Kim, 2013), suggesting that customers tend to opt for a new service only when the investment -- monetary and non-monetary – offers more than marginal benefits.

- **Perceived benefits**

Hsu and Lin (2016) highlight the perceived benefits as a significant determinant of user attitude towards IoT services. In Kim, Park and Choi (2017), the Elaboration Likelihood Model is used to identify usefulness, enjoyment and facilitating conditions as predictors of perceived benefits.

- **Facilitating conditions**

The most important determinant of perceived benefit identified in (Kim, Park & Choi, 2017) are the **facilitating conditions**. Facilitating conditions are defined in **(Kim, Park & Choi, 2017)** as the "degree of belief in the organizational and technical infrastructure", inspired from (Davis, 1989) and (Venkatesh, Thong & Xu, 2012).

- **Perceived sacrifice**

Privacy risk was found to be the most influential determinant on perceived sacrifice in (Kim, Park and Choi, 2017). In addition, innovation resistance, technicality as well as perceived fee had an influence on perceived sacrifice.

- **Perceived reliability**

Yang, Lee and Lee (2018) consider service stability, security, and privacy as critical factors for acceptance of smart home services. These factors are grouped under the term 'reliability'. Safety, security and protection are the second needs to be satisfied in the Maslow pyramid, after basic physiological needs (Maslow, 1943). Hence, they are of utmost importance when considering smart home adoption. In (Chan et al., 2008), reliability of sensors and data processing systems are considered as important determinants of smart home adoption. Technical errors can be a concern to smart home users; hence the technology should not malfunction. In addition to not malfunctioning, the technology should provide accurate services that are flawless (Yang, Lee and Lee, 2018). Users' trust in smart home service providers is also key to the diffusion of smart home services (Yang, Lee & Lee, 2018).

Privacy is defined in (Shin, Park & Lee, 2018) as "the user's concern about the infringement of personal information that occurs while using a service" and is found to be a statistically significant predictor of attitude for female users, but with small effect size. In Kim, Park and Choi (2017), the determinant that had the most influence on perceived sacrifice was found to be privacy risk, hinting to privacy issues as a major barrier to smart home adoption. Security and privacy are often mentioned as barriers to smart home adoption in the literature (e.g. Tanwar et al., 2017; Obaidat, 2017; Balta-Ozkan et al., 2013; Bao et al., 2014).

- **Perceived enjoyment**

Kim, Park, and Oh (2008) found perceived enjoyment to be a determinant of perceived usefulness in mobile services use. However, when tested in (Park et al., 2017), perceived

enjoyment was not significant to predict perceived usefulness of smart home services. Rogers, Bagozzi and Warshaw (1992) define perceived enjoyment as “the degree of which using IoT technologies in smart home environments is considered to be pleasurable and playful”.

- Perceived ease of use

In (Park et al., 2017), perceived ease of use is influenced by perceived control, perceived compatibility and perceived connectedness. In (Shin, Park & Lee, 2018), the effect of perceived ease of use on attitude is found to be different depending on age and gender. In the senior age group, perceived usefulness has a greater influence on attitude than ease of use. This is consistent with the TAM 3 (Venkatesh & Bala, 2008) but inconsistent with (Park et al., 2017), where the effect of perceived ease of use on attitude is twice as large as perceived usefulness on attitude. However, in the junior group the effect of perceived usefulness on attitude is substantially lower than the effect of perceived ease of use on attitude (Shin, Park & Lee, 2018).

- Perceived usefulness

In (Park et al., 2017), perceived usefulness is very well explained (95% of the variance) by perceived connectedness, perceived ease of use, and particularly perceived compatibility. Shin, Park and Lee (2018) find that perceived usefulness has more influence on attitude for men than women, for the senior age group than the junior age group, and for the lower income group than the higher income group.

- Perceived automation

Automation was a key feature in the previous generations of smart homes and has now become more affordable, simpler and smarter (Yang, Lee & Lee, 2018). AI technology has allowed home automation to become higher-level by assisting its users in a more intelligent way (Reinisch, Kofler & Kastner, 2010). Luor et al. (2015) highlighted the link between home automation and user attitude. However, in (Yang, Lee & Lee, 2018) automation is found to be not significant in explaining user intention to adopt a smart home. They suggest that people are rather searching for safer and more effective home automation systems than highly advanced systems. This can itself be explained by the users prioritizing control and safety over

their home, which is their personal space. Hence, the amount of automation expected by users seems to be limited and depending on personal user characteristics and environment.

SECTION 2 – PRACTICAL PART

CHAPTER I - RESEARCH GOALS

After having reviewed the literature, in this part, we set some more specific goals concerning the outcomes we would like to reach with our research. As it has been stated earlier, this work aims at providing guidance to practitioners of the IoT-enabled smart home market in order to have their services and/or products adopted by the consumers. We aim to reach this main goal by following two broad steps.

The first step is to identify the important factors affecting consumer adoption of IoT-enabled smart homes, hence a first research question is: *"What are the main determinants of consumer adoption of IoT-enabled smart homes?"*. This step corresponds to a rather theoretical approach and serves as support for the next step.

Then, the second step consists of transposing the knowledge built from the first step into practical guidance, through a framework, that can be applied by domain professionals. Therefore, a second research question we try to answer is: *"What are the practical interventions managers of IoT-enabled smart homes can take in order to foster consumer adoption of smart homes?"*.

CHAPTER II - ANALYSIS MODEL

As aforementioned, the approach adopted in this work is divided into two steps: identifying the main determinants of IoT-enabled smart home adoption and developing a framework that can serve as practical guidance for managers.

In the literature, some barriers and challenges to smart home adoption have already been highlighted. Other potential determinants of IoT technology and smart home adoption have also been mentioned earlier. All these elements serve as basis for constructing our framework.

Our methodology consists of: developing and testing a model explaining the determinants of IoT-enabled smart home adoption; extracting insights from a survey; developing in-depth insights on smart home use, gathered from semi-structured interviews with smart home users and potential users; and building a framework for possible intervention guidelines to support practitioners.

More specifically, we conduct an online survey to gather insights on smart home adoption from the demand-side. Data exploration is done on the answer data and insights are drawn from there. In addition, some of the answers are used for developing the adoption model. Semi-structured interviews are also led, with smart home users. Finally, all the insights drawn from the different approaches (i.e. online survey, model, semi-structured interviews, and literature review) are gathered together and integrated into an unified framework proposing clear and practical guidelines to support the management board of smart home service and/or product providers.

2.1 Online survey

2.1.1. Online survey description

The aim of the survey is to compare the theoretical elements that we have reviewed with current and potential customers of connected objects and smart homes. Understanding the expectations and fears of potential customers regarding technology is crucial for its widespread adoption. The main objective of the survey is to verify the early adopter profile

and to assess which elements may have an influence on the buying process of smart devices or smart homes. Some questions of the survey are also used in developing our adoption model. The analysis of the respondent's answers will allow us to give practical advices to companies wishing to enter the smart home market on the basis of the needs, desires and recommendations addressed by potential customers in our survey.

2.1.2. SURVEY METHODOLOGY

Two surveys were made using the same questions, one in French and the other one in English. The surveys were created using Google Forms. They were open to people aged ≥ 18. The surveys were diffused by emails and on two different social medias namely Facebook and Linkedin. In order to build insights into smart home adoption, we required more answers from smart home users. Therefore, we reached out to them by diffusing the English-speaking survey on smart home dedicated online forums, essentially on Reddit/SmartHome (https://www.reddit.com/r/smarthome/) and other smart home related 'subreddits'. Both surveys can be found in the appendix section of this work. The surveys were accessible for two weeks. The online survey contained both open and closed questions and started with a definition of the terms 'smart home' and 'smart devices' in order to make sure respondents understood the questions mentioning these terms well. Most questions used a five-point Likert-type scale to define the importance rate, the acceptance rate, or the influence (potential) customers give to different factors (These results can be found as Appendix 3).

2.1.3. BENEFITS & DRAWBACKS OF THE METHOD

In their book titled "Marketing Stratégique et Opérationnel", Lambin and de Moerloose (2016) list the different advantages and drawbacks of survey instruments. Here is a table highlighting the most prevalent ones for online surveys in the context of our work.

Benefits	**Drawbacks**
Fastest method and very inexpensive	Non-random sampling: numerous refusals/replies

Possibility of worldwide coverage	Processing software (Google Forms) limiting the choice of possible scales
Possibility of control over the order of questions	Poor control of the identity of respondents
Immediate encoding	Impersonal contact
Ability to use a visual aid	Fear of invasion of privacy when confidentiality cannot be ensured
Absence of bias due to the investigator physical presence	

Table 7 - Advantages and drawbacks of online surveys based on (Lambin & de Moerloose, 2016)

2.2. Adoption Model

Concerning our adoption model, the main determinants were identified based on the literature and our own reflection. We chose to develop a smart home extended version of the TAM because: the TAM is a very commonly used model to explain an individual's acceptance of a technology, it was empirically validated by Davis (1989) and other works afterwards, and it has been backed by a wide amount of reviews and empirical research (e.g. Hu et al., 1999; Moon & Kim, 2001). It is also a simple (small number of factors) and understandable model, based on causal links, that allows us to have a good overview on smart home adoption. This is an important factor to keep in mind since the overall focus of this work is to identify managerial implications, hence the TAM is used as a mean to achieve that goal rather than a goal in itself. The TAM's factors are simple yet specific, easy to use and easy to understand

This work uses the TAM as model because: it is commonly used to explain an individual's acceptance of a technology because, it was empirically validated by Davis (1989), it has been backed by a wide amount of reviews and empirical research (e.g. Hu et al., 1999; Moon & Kim, 2001), it is simple (small amount of factors), it is applicable to a wide variety of contexts, and the factors used are simple, specific, easy to use and easy to understand.

The model was developed and tested using a Structural Equation Modeling Technique (SEM). SEM is also referred to as causal modeling, causal analysis, simultaneous equation modeling, or analysis of covariance structures. Path analysis and confirmatory factor analysis are two types of SEM that are also often mentioned (Ullman & Bentler, 2003). SEM techniques allow to examine a set of relationships between one or several independent (continuous or discrete) variables as well as one or a set of dependent (continuous or discrete) variables (Ullman & Bentler, 2003). Causal links are created and tested between the different factors. Factors are also called latent variables, constructors, or unobserved variables. Another useful aspect of SEM is the visual representation of the path diagrams, as they help clarifying the causal links, hence hypotheses, between factors. SEM allows to test complex and multidimensional relationships, and all at the same time. Another advantage of this type of model is the possibility of having latent variables being predicted by other variables (i.e. dependent variable) as well as predicting other variables (i.e. independent variable).

Factors, or latent variables, are by definition, variables that cannot be directly measured. Hence, they're indirectly constructed by combining one or more measurable variables together, called indicators. In our case, the measurable variables (indicators) were measured by the answers to the online survey questions. Those answers corresponded to a five-point Likert-type scale. In other words, each question provides a measured variable (i.e. answer of the respondent) that is then combined with other similar measured variables in order to either form or reflect the latent variable (see further for reflective and formative relationships). For instance, the latent variable 'intention to use' is inferred by combining the answers (measured variables) to two different questions related to a user's intention to use a smart home. Measured variables are also called observed variables, indicators, or manifest variables.

The SEM approach and its factors' relationships is computed by using Partial Least Squares (PLS) regression, a path modeling method first developed by Wold (1982). PLS-SEM (PLS Structural Equation Modeling), also called PLS-PM (PLS Path Modeling), is a quite recent and emerging statistical method. Hair et al. (2014) identify the main justifications for the use of PLS-SEM in business research as: their ability to deal with non-normal data, the small sample sizes required, and formatively measured constructs. Chin, Marcolin, and Newsted (2003) also noted that PLS has minimal restrictions in terms of distributional assumptions and sample

size. PLS-SEM has the advantage of being a “soft modeling” method where fewer hypotheses on distribution are made and a lower sample size is required, in comparison to the “hard modeling” method (often called LISREL) developed in Jöreskog (1970).

PLS-SEM models consist of two models: a measurement model (or outer model) where the indicators are linked with their corresponding latent variable, and a structural model (or inner model) where the different factors are linked to each other, hence their relationships are hypothesized. In the measurement model the links between indicators and factors can be either formative or reflective. With reflective links, the indicators are supposed to reflect the corresponding latent variable through a simple regression, where the residual is hypothesized to have a mean of zero and to be uncorrelated to the latent variable. Reflective links are used when several indicators can be interchanged with each other without affecting the corresponding latent variable. Hence, there is a strong correlation between the reflective indicators of a latent variable. EFA (exploratory factor analysis) can be used to identify those strong correlations and find the right reflective indicators of a latent variable.

Formative links between indicators and the latent variable highlight a link where the indicators help construct the latent variable, instead of reflecting it. Hence, they are related to each other to some extent, as they help forming the latent variable, but are not necessarily strongly correlated with each other. The block of indicators can be multidimensional. Hair et al. (2016) highlight the common belief in the superiority of using PLS-SEM for formative links, in comparison to CB-SEM. PLS-SEM is considered by many as the recommended modeling method to that regard. However, it must be insisted that the criteria to evaluate the formative indicators is totally different than the ones for the reflective indicators (Hair et al., 2014). For more information on PLS-SEM we refer to Chin (1998), Tenenhaus et al. (2005) and Hair et al. (2016). In addition, Hair et al. (2016) also provide an extensive review of the different steps that need to be undertaken when using PLS-SEM.

This work follows the different stages suggested in Hair et al. (2014) and Hair et al. (2016), that are: model specification, outer model (measurement model) evaluation, and inner model (structural model) evaluation.

2.2.1. MODEL SPECIFICATION

In the model specification, both the inner and outer models need to be set up. This is first done by looking at previous research and using some logic to develop the relationships between the different latent variables. Latent variables (or constructs) are either endogenous or exogenous. Exogenous latent variables act as dependent variables whereas endogenous latent variables act as independent variables but can also act as dependent variables when put as intermediate between two other variables. Second, once the inner model is set up the outer model needs to be set up. It must be decided on whether a one-item or multi-item scale will be used (Diamantopoulos et al., 2012; Sarstedt and Wilczynski, 2009) as well as either a formative or a reflective link will be used (Diamantopoulos and Winklhofer, 2001; Gudergan et al., 2008). Good specification of the outer model is crucial as the hypotheses made in the inner model can only be as valid and reliable as the outer models (Hair et al., 2014).

2.2.2. OUTER MODEL EVALUATION

Once both inner and outer models have been specified, it is necessary to run the PLS-SEM algorithm a first time in order to evaluate the results, in terms of reliability and validity, of the outer model. Reliability and validity of the latent variables can be assessed in several ways.

As reflective indicators are expected to accurately reflect the conceptual domain of the factor, they are interchangeable and highly correlated. Hence, the group of indicators is said to be unidimensional. Reflective indicators are connected to a factor through loadings. Loadings correspond to the bivariate correlations between the factor and the indicator (Hair et al., 2014). When assessing the reliability of reflective indicators, composite reliability can be used in favor of Cronbach's alpha as it doesn't assume all indicator loadings to be equal (i.e. takes into account differences in factor loadings) and the number of items in the scale does not affect the internal consistency reliability. Cronbach's alpha also tends to underestimate the internal consistency reliability. Concerning the validity of reflective indicators, an average variance extracted (AVE) of minimum 0.5 should be targeted as well as outer loadings above 0.70 (Hair et al., 2014). Then, it needs to be verified that the factors are empirically distinct from each other. Discriminant validity can be verified in different ways. One way to do is by using the Fornell and Larcker (1981) criterion where it is tested that the

factor shares more variance with its indicators than with any other construct. In practice, this is verified when the AVE of each factor is higher than the squared correlation with any other factor (Hair et al., 2014). Another way to test discriminant validity is by verifying that the cross loadings of each indicator on its factor are higher than the cross loadings on other constructs.

As mentioned earlier, formative indicators do not share the same properties as reflective indicators. Hence, they should be evaluated with different criteria than the latter. First, content validity should be assessed. Content validity refers to the extent to which indicators capture the main aspects of the factor. If an indicator of a particular aspect of the factor is omitted, the whole factor may be altered (Diamantopoulos et al., 2008). Convergent validity should be evaluated, which can be done through a redundancy analysis comparing the correlation of a factor with an alternative reflective or single-item measurement of the same factor (Hair et al., 2016). Besides content validity, collinearity must also be tested as a high collinearity could bias the results. Significance and relevance of each formative factor should also be verified. To that regard, bootstrapping is used to determine the level of significance of each indicator weight. When bootstrapping, the original data is used to generate a large amount of subsamples, where models are estimated for each subsample. These model estimates are then used to compute a standard error for each model parameter, which is then used to compute the significance of each indicator, through the t-statistic (Hair et al., 2014). Concerning the relevance of the indicators, the weights assigned to each factor-indicators relationship indicate the relative contribution of the indicator to forming the factor (Hair et al., 2016). When the relationship is nonsignificant, the decision to whether exclude the indicator or not from the measurement model should be taken by analyzing the bivariate correlation (loading) between the indicator and the factor (Hair et al., 2016). This is rather uncommon as omitting an indicator implies omitting a conceptual part of the factor.

2.2.3. INNER MODEL EVALUATION

After evaluating the outer model, it is required to evaluate the inner model, containing the previously hypothesized relationships between factors. The PLS-SEM will compute the parameters that give the best prediction of the endogenous constructs. There is no standard statistic to assess of the model fit of PLS-SEM (Henseler & Sarstedt, 2013). However, several statistics allow to evaluate the model's ability to predict exogenous variables. These statistics

include the coefficient of determination (R2), cross-validated redundancy (Q2), path coefficients, and the effect size (f2). Before using these statistics, collinearity between factors must be verified and removed. The Fornell-Larcker criterion can be used for detecting collinearity in the inner model, except when dealing with formatively constructed factors. Related to the statistics that can be used to assess the model's ability to predict the exogenous variables, the adjusted R2 should be favored to the standard R2. The (adjusted) coefficient of determination R2 reflects the combined effect of the exogenous variables on the endogenous variable(s). The adjusted R2 penalizes the model (by reducing the adjusted R2) when additional factors are added to the model, as they will always increase the R2 as long as they are slightly correlated with the endogenous variable, even if the link is not meaningful (Hair et al., 2014). A general rule of thumb is concerning the value R2 should take is 0.25 for a weak level, 0.5 for a moderate level, and 0.75 for a strong level of prediction accuracy (Hair et al., 2011; Henseler et al., 2009). However, this greatly depends on the domain of application.

Inner models can also be assessed using the cross-validate redundancy (Q2). The Q2 compares predicted parameter models, estimated on a subset of the data, with the original values that were omitted in the data subset used to estimate the parameters. When the Q2 value for an endogenous factor is higher than zero, it indicates that the relationship is relevant from a prediction point of view. However, it does not indicate the quality of the prediction (Rigdon, 2014; Sarstedt et al., 2014).

Concerning the path coefficients, which correspond to the effect size of a hypothesized relationship between two factors, estimates can be obtained by running the PLS algorithm on the model. The significance of these relationships can be checked with the t-statistic, obtained by bootstrapping (Helm et al., 2009). It should also be checked if the obtained path coefficients actually make sense (Hair et al., 2016).

Another useful statistic is the effect size (f2). The f2 is computed by observing the change in R2 when a particular factor is removed from the model. An f2 value of respectively 0.02, 0.15, and 0.35 represent small, medium, and large effects (Cohen, 1988). In other words, when the change in R2 is high when removing a particular factor of the model, then f2 will be high, meaning the exogenous factor strongly contributes (i.e. has a large effect) to explaining the endogenous factor.

2.3. INTERVIEWS

2.3.1. INTERVIEW DESCRIPTION

We were fortunate enough to be able to conduct 3 interviews. The interviews were conducted in French with a smart home owner, a person who is enthusiastic about this technology but did not embrace it yet and a person who is reluctant to have a home with connected objects. We made this decision because we think it's interesting to understand why some people are convinced by this technology, why some may be enthusiastic and still hesitate to take the step and why others are totally opposed to it. Because of the ongoing global pandemic, we have had to rely on our relatives and acquaintances to conduct these interviews and we are aware that this may introduce a bias in our interviewee's responses. Nevertheless, we believe that the insights provided by these interviews outweigh the potential selection bias. In addition, the health crisis forced us to conduct online interviews using a video conferencing platform sometimes making the conversation less natural.

2.3.2. INTERVIEW METHODOLOGY

Interviews are a commonly used method of collecting qualitative information and also allows us to mitigate and counterbalance the drawbacks of the online survey described just above. Thanks to interviews, it is possible to get immediate answers from an individual on a particular topic. In addition, verbal interactions usually lead to more complete answers and also allow the interviewee to ask questions to make sure that his or her answer was understood as he or she meant it. Finally, the body language present in an interview can also provide interesting leads and insights regarding the research objective (DeCarlo, 2018).

In the context of our work, we decided to opt for qualitative semi-structured interviews following the framework proposed by (Kallio et al., 2016).

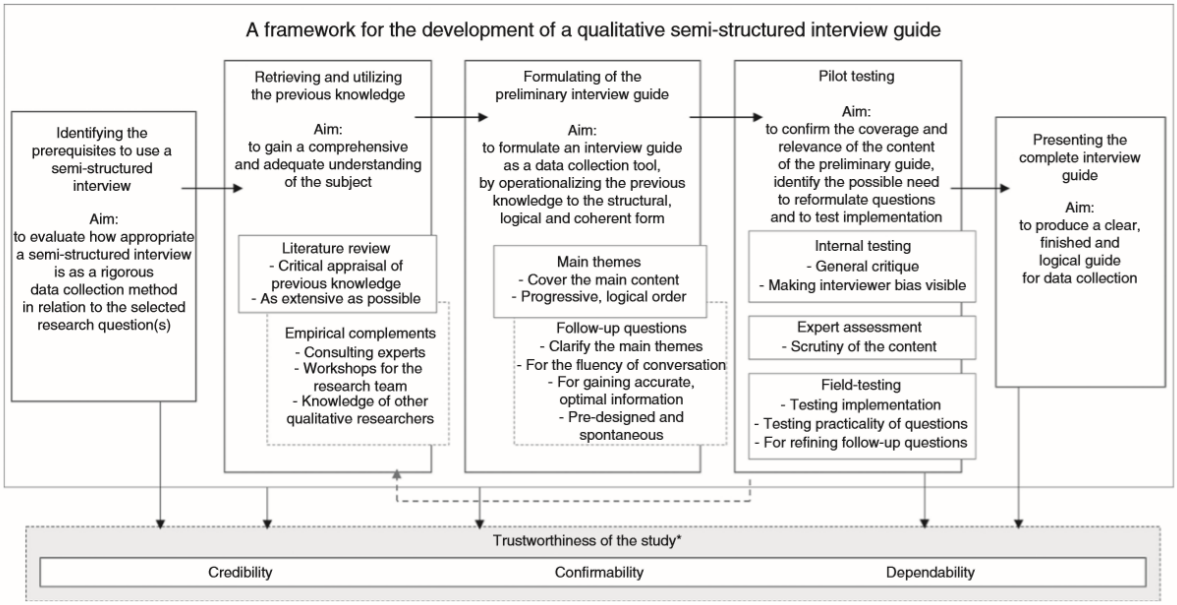


Fig. 6 - The phases of a semi-structured interview guide by Kallio et al. (2016).

Qualitative interviews, also often referred to as in-depth or intensive interviews, are semi-structured. The question asked are open-ended as the purpose is to hear from respondents about what they believe is useful for the research at hand and express their expert advice with their own words. These qualitative interviews require an interview guide which is a list of topics and questions the interviewer wants to cover during the interview and is used to guide the conversation for it to be as insightful as possible. In addition, questions and topic are not set in stone and may differ according to the interviewee expertise, interest or behavior during the interview.

2.3.3. ADVANTAGES AND DISADVANTAGES OF THE METHOD

The positive points of the methodology used have already been partially covered in the first paragraph of this part. Another, worth mentioning benefit of semi-structured qualitative interviews, is that any topic can be explored in much more depth with interviews than with almost any other method (e.g. Online Survey research).

Nevertheless, the method also has some flaws that have to be mentioned. First of all, conducting this type of interview is a time consuming and demanding process for both the researcher and the interviewee. In addition, qualitative interviews rely on “respondents' ability to accurately and honestly recall specific details about their lives, circumstances, thoughts, opinions, or behaviors which is difficult to guarantee” (DeCarlo, 2018). Finally, another risk of this method is that some questions in the interview guide contain an implicit bias we would not have noticed and that would unconsciously guide the participant's response in a particular direction.

CHAPTER III - DATA COLLECTION, OBSERVATION AND MODELLING

3.1. Online Survey

The data collection was done directly on Google Forms, however, the final file was exported in CSV format on an Excel spreadsheet in order to start the exploration of the collected data. Having produced 2 similar surveys but in different languages, the two datasets were merged on Excel so that we could observe general results. In the end, 135 responses were collected. The sample will be detailed in the section "Analysis" section coming next.

3.2. Adoption Model

3.2.1. Model specification

First, it is required to construct the inner model by identifying its factors and hypothesizing their relationships. As mentioned earlier, the model that is presented in this work is an adapted version of the TAM to the IoT-enabled smart home. Based on previous research on both the TAM as well as smart home specific TAM models (see review of the literature), and in addition to our own reflection, we suggest several factors and their relationships with each other. As this work aims at identifying the main managerial implications, this model tries to identify the main factors that can affect the user intention to adopt an IoT-enabled smart home.

The indicators used in this model have been obtained through the online survey, that was presented earlier in this work and that is accessible in Appendix 1. Before setting up the survey, the factors that would be studied and used in the model were identified and the hypotheses concerning their relationships were made. In this section, those factors and their respective hypotheses are presented.

First, the main factor in this model is the intention of users to adopt an IoT-enabled smart home and its services. This is the variable that the model tries to explain by developing the formative links that lead to that latent variable.

Second, attitude corresponds to the general impression users have of smart homes. In the first version of the TAM, Davis, Bagozzi and Warshaw (1989) already identified attitude as a determinant of a user's intention to use a technology. They stated that "all else being equal, people form intentions to perform behaviors toward which they have positive affect". We believe that this applies to the specific smart home adoption and suggest that positive attitudes towards smart homes should have a positive influence on a user's intention to adopt a smart home. Hence, we propose the following hypothesis:

H1: Attitude is positively associated with smart home adoption intention.

Third, perceived ease of use is defined as "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989). We suggest that when confronted to a smart home system, the easier the user perceives the usage of the system, the more favorable his attitude will be towards using the system. In parallel, if the use of a system is perceived as difficult, the user will lose motivation in using the system and will develop negative attitudes towards the system. Hence, we posit that:

H2: Perceived ease of use is positively associated with attitude towards smart home adoption.

We also analyze the perceived ease of use as determinant of perceived usefulness. This relationship has already been validated in a vast amount of previous works (e.g. Venkatesh & Bala, 2008; Venkatesh & Davis, 2000) and serves as basis of the TAM. The rationale thinking behind this is that if the user finds it easier to use the smart home system, the less effort it will require, and the more useful it will become. Further, the more experience the user will

have with the system, the easier it will be for him to use it, hence the more useful it will become. Therefore, we set the following hypothesis:

H3: Perceived ease of use is positively associated with the perceived usefulness of a smart home system.

Fourth, perceived controllability refers to the ability of the system to allow the user to do whatever he needs with the system. Remote control is an important feature of the controllability of the smart home as it allows the system to be controlled from anywhere and at any time (Yang, Lee & Lee, 2018). We suggest that controllability, through an intuitive and well-conceived user interface and remote control, should make facilitate the use of the system for a user. Hence, we posit that:

H4: Perceived controllability is positively associated with the perceived ease of use of a smart home system.

Fifth, perceived compatibility is used to assess "how smart home services are interoperable with various home appliances and external services" (Shin, Park & Lee, 2018). When devices are able to communicate and exchange data with each other, services such as automation should become more effective, hence the overall performance of the system is expected to improve and therefore its usefulness as well.

Therefore, we posit that:

H5: Perceived compatibility is positively associated with the perceived usefulness of a smart home system.

Compatibility with other devices is also identified in the literature as a key challenge for smart home adoption. If this challenge can be overcome, users would be able to control all their devices through a single common interface, making it much easier and practical to control the system. Hence, we hypothesize that:

H6: Perceived compatibility is positively associated with the perceived ease of use of a smart home system.

Other works (Shin, Park & Lee, 2018; Park et al., 2017; Tsai, Chien & Thai, 2014) have highlighted the relationship between perceived compatibility with perceived usefulness and perceived ease of use of smart home systems.

Sixth, perceived usefulness is defined as "an instrumental belief that is conceptually similar to extrinsic motivation and is a cognition (as opposed to emotion) regarding the benefits of using a system" (Venkatesh & Bala, 2008). Drawing from the initial definition of Davis (1989) we define perceived usefulness as the degree to which a person believes that using a particular system would better assist him. We believe that when people better perceive the benefits of using the system as well as its relevance the user's intention to adopt a smart home should be positively influenced. Hence, we make the following assumption:

H7: Perceived usefulness is positively associated with the user's intention to adopt a smart home system.

This hypothesis has, to our knowledge, always been verified in previous literature on smart home adoption.

Seventh, perceived enjoyment is defined, based on Rogers, Bagozzi and Warshaw (1992), as "the degree of which using IoT technologies in smart home environments is considered to be pleasurable and playful". Perceived enjoyment is identified by Venkatesh (2000) as an anchor of perceived ease of use. Thus, perceived enjoyment helps users form early perceptions on the ease of use of a smart home system, based on their own general beliefs regarding a smart home and its use. As in Venkatesh (2000) and Venkatesh and Bala (2008), we believe that these initial anchors (i.e. initial beliefs and judgements) are adjusted with the users' personal hands-on experience, and perceived enjoyment is supposed to increase. We therefore suggest that:

H8: Perceived enjoyment is positively associated with the user's perceived ease of use of a smart home system.

Eight, it is important to also take into consideration the main sacrifices done by users when adopting a smart home. While we have hypothesized that perceived usefulness and perceived ease of use (through attitude) positively influence user intention, we also believe that some major concerns and sacrifices prevent users from adopting smart homes. Including sacrifices

in the model is mainly driven by the fact that the TAM is purposed for organizational use where its use is borne by the organization and its costs for the user are taken into account by the original TAM only to a limited extent. For instance, no monetary costs are imputed to the user in the organizational context, hence they're not included in the TAM. As a smart home system's use is only encouraged by its occupants and the sacrifices related to its use are directly imputed to the users, we suggest that sacrifices should be taken into account when users form their intention to adopt such system. The conceptual domain of the sacrifices is very wide and therefore formative indicators are used, in contrast to the reflective indicators that were used for the other factors of the model. The main sacrifices (monetary and non-monetary) we identify are: privacy risks, the loss of control and dependence on technology, as well as the perceived fee. We believe that these sacrifices have a negative influence on the users' intention to adopt a smart home system and therefore posit that:

H9: Sacrifices are positively associated with the user's intention to adopt a smart home system.

Once the inner model developed, it is required to develop the outer model by identifying the indicators as well as the way they will be measured. For the purpose of this model we used a five-point Likert-type scale to measure the indicators. Most questions were asked to all the respondents of the survey (non-users as well as users). However, as some questions required a deeper understanding and experience with a smart home, these were only asked to smart home users. In order to make sure non-users as well as users had a common understanding of what a smart home and smart devices were, both terms were defined at the beginning of the survey.

3.2.2. OUTER MODEL EVALUATION

After collection of the results, the outer model had to be tested. The several test criteria and their results can be found in Appendix 4. In order to achieve those results, the several indicators that were in the initial model but did not match the criteria were removed.

In some cases, several indicators had to be removed which, in the case of the perceived compatibility factor, led to only one reflective indicator. However, for other factors at least two indicators were used for each factor.

The software used to test and verify the model was SmartPLS 3 (Ringe, Wende & Becker, 2015). The PLS algorithm was applied, using the path weighing scheme, a max amount of 2000 iterations and a stop criterion of 10^{-7}. For what concerns the bootstrapping method, 2000 subsamples were randomly selected, the "basic bootstrapping" method was applied with Bias-Corrected and accelerated (BCa) bootstrap, with a two-tailed test type.

Reflective indicators were tested by looking at the loadings as well as the reliability and the validity of the factors. As presented earlier, reflective indicators are connected to a factor through loadings.

The reliability of those loadings can be estimated by looking at their composite reliability. Other criteria (e.g. Cronbach's alpha) can also be used but seem less appropriate. These different criteria and the obtained results can be found as Appendix 4. It is important to note that, after several tests, only one indicator was validated for the perceived compatibility factor. It is also important to remember that all indicators were reflective indicators, except for sacrifices. Looking at the results, it can be observed that the composite reliability of the factors is above 0.70 in all cases. Hence, the reliability is validated. However, it is important to point out that the Cronbach alphas are particularly low in some cases. Potential explanations of this have already been mentioned earlier.

	COMPOSITE RELIABILITY	AVE
ATTITUDE	0.741	0.595
INTENTION TO ADOPT	0.825	0.702
PERCEIVED COMPATIBILITY	1.000	1.000
PERCEIVED EASE OF USE	0.729	0.575
PERCEIVED ENJOYMENT	0.778	0.639

PERCEIVED USEFULNESS	0.945	0.896
PERCEIVED CONTROLLABILITY	0.848	0.738
SACRIFICES		

TABLE 7 - Observed Composite Reliability and Average Variance Extracted (AVE)

In Table 7 it can be observed that the average variance extracted (AVE) is above the targeted 0.50 for all factors. However, not all the outer loadings are above 0.70, as was suggested by Hair et al. (2014). The values of 0.64 and 0.683 are still close to this target and since the target value of 0.70 is more for comparison as an exclusion, we find it more relevant to keep those indicators than to remove them from the model. Hence, the overall validity of the factors is validated. In addition, it must be looked into the discriminant validity as we want to ensure that the factors are empirically distinct from each other.

Discriminant validity can be verified in different ways. One way to do is by using the Fornell and Larcker (1981) criterion where it is tested that the factor shares more variance with its indicators than with any other construct. In practice, this is verified when the AVE of each factor is higher than the squared correlation with any other factor (Hair et al., 2014). The Fornell and Larcker criterion was successfully tested (see Table Appendix 4) and validated. Moreover, it was tested whether the cross loadings of each indicator on its factor would be at least 0.20 higher than with any other factor. This discriminant validity test was also conclusive. Hence, the reflective indicators of the outer model were tested, and the factors' reliability and validity validated, as well as the discriminant validity.

For what concerns the formative indicators of sacrifices, collinearity was tested by looking at the VIF values. Sacrifices' indicators VIF values were comprised between 1.106 and 1.309, validating the collinearity test (see Appendix 4). Significance of the formative indicators' weights was also tested, after bootstrapping. It appeared that none of the indicators' weights were significant at a level of 0.05. Concerning the loadings, only one of the indicators was found significant at a level of 0.05. However, we decided to not reject these indicators immediately, as removing those indicators would remove a conceptual dimension of

sacrifices. We will keep an eye on this issue when analyzing the inner model, as the inner model is directly affected by the quality of the outer model.

3.2.3. INNER MODEL EVALUATION

Concerning the inner model evaluation, several statistics were computed (Appendix 5).

First, it was checked whether multicollinearity was present between two factors. All VIF values obtained were around 1.0, hence no multicollinearity between the factors was observed.

Second, the adjusted coefficients of determination (adjusted R2) obtained can be observed in Figure 7. The obtained adjusted R2 for the intention to adopt a smart home is of 0.287. This value is relatively low, hinting that more factors might affect the intention to adopt. When looking further, it appears that the perceived ease of use is not represented very well in the model, with a weak level of prediction accuracy.

The cross-validated redundancy (Q2) showed that all the factor relationships are relevant as they were higher than zero.

Path coefficients also need to be analyzed. We refer to figure 7 for the significance of the paths. Unsurprisingly sacrifices have a negative influence on adoption intention. However, this relationship is not proved to be significant. The relationships between perceived ease of use with both attitude and perceived usefulness are very strong and significant at a level of 0.05. Perceived enjoyment is found to have a strong (and significant at a level 0.05) influence on perceived ease of use. Attitude has also a strong (and significant) effect on intention to adopt. Perceived usefulness' effect on intention to adopt is not found significant at a level of 0.05, but is significant at a level of 0.10.

For what concerns the effect size (f2), the f2 values (see Appendix) highlight that perceived compatibility has a low effect and might be removed from the model without much affecting the R2. The same applies to perceived controllability. In contrast, removing perceived ease of use would have a high impact on the model.

While perceived ease of use seems to be poorly predicted (with a very low adjusted R2) it appears to have a very strong influence on perceived usefulness as well as attitude.

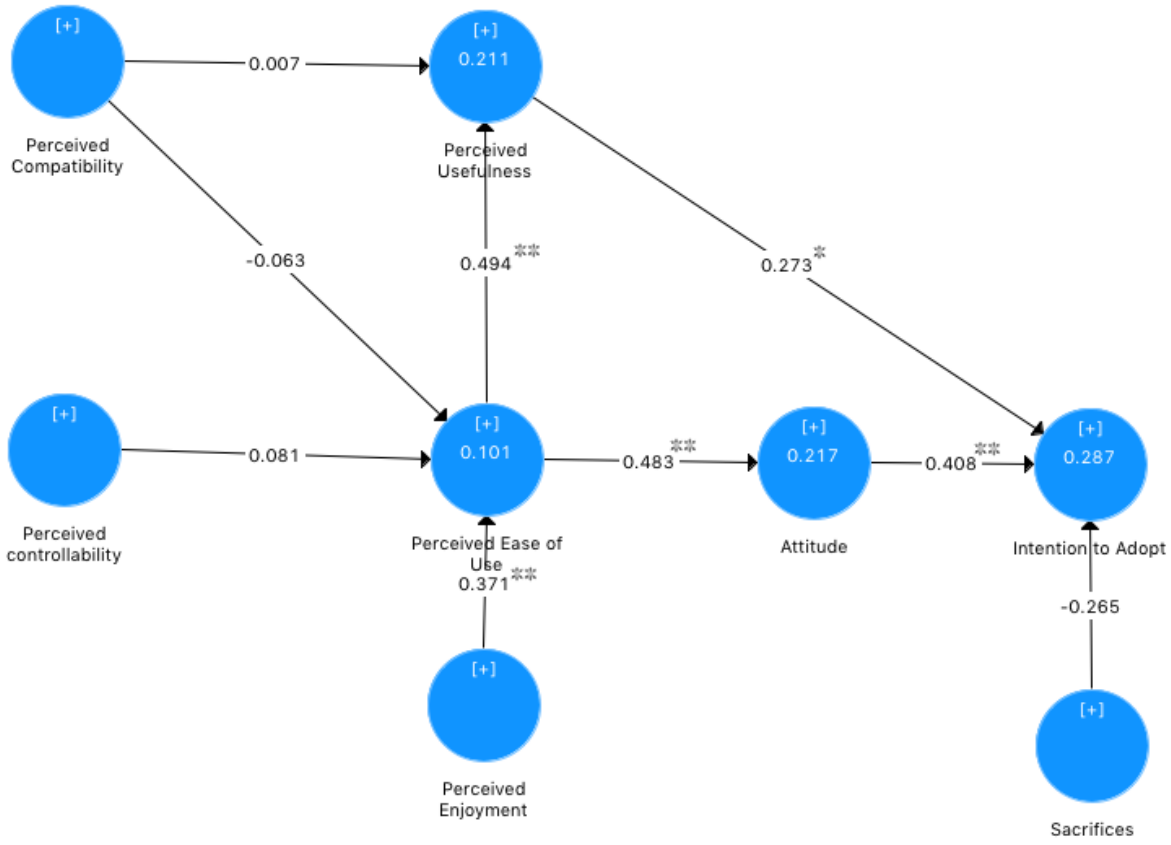


Fig. 7 - Smart Home Adoption Model with path coefficients and significance at a 0.05 level (**) and 0.10 level (*)

3.3. Interviews

Data collection is a very important part during an interview as it constitutes the first step of the data analysis (DeCarlo, 2018). Having the chance to work in pairs, we assigned ourselves a role. During the interviews, one of us would take notes while the other one interacted with the interviewee in order not to lose eye contact and to take into consideration the interviewee's body language. In addition, in order to ensure that important information was not missed during the analysis phase, the audio of the interviews was recorded with the participant's consent.

CHAPTER IV – ANALYSES

4.1. INSIGHTS DRAWN FROM THE ONLINE SURVEY

In this section, we will first describe the overall sample and give its main characteristics. We will then describe the sub-sample of smart home owners in more detail before analyzing the results of this online survey.

A total of 135 participants (40 female and 95 male) participated in this online survey. All participants were volunteers and have different backgrounds. The typical participant (persona) is a man aged 25-34 (25.93%) or 45-54 (25.19%) and lives in Belgium (63.70%) or the United States (21.48%), in a household of 3 or more people (57.04%). He has a developed interest in new technologies in general (91.85%) and already owns 5 or more connected objects (53.33%). He is owner of a house (67,41%) and has an income of more than 2298€ per month (69,63%). His home is not connected (63.70%) and located in an urban area (54.81%). He is considering the acquisition of a connected home in the future (73.33%) for which he would be willing to pay 1 to 5% more of his purchase budget (48,89%). Finally, he would prefer to proceed to a one-time payment rather than a monthly subscription for his smart home (63,70%) and does not know any Belgian company active in the field of connected objects or the smart home (96.30%).

Our survey also allowed us to test the respondents' interest in the 6 sub-sectors of home automation that we discussed earlier in the section "Market Overview & Opportunities". The sub-sector driving the most interest is Home Control devices (88% of the 135 participants) closely followed by Energy Management (86%). Security devices comes third (83%) and Lighting and Comfort comes fourth (79%). Finally, the Home Entertainment (69%) sub-sector and the smart appliances sub-sector (53%) come last.

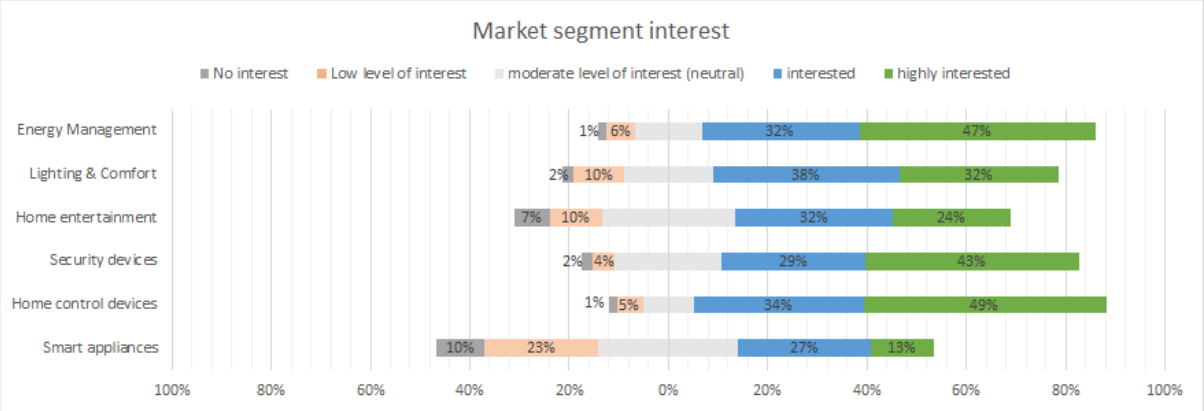


Fig. 8 - Likert plot depicting survey results on market segment interest of survey respondents.

Thanks to this survey, we also tested the importance of certain factors on the purchase intention of potential customers towards a connected object designed for home automation purposes. Among the tested elements, the convenience comes first (84%) followed by the privacy granted to private data (81%). Other factors such as security against hacking (78%), price (75%) and compatibility (74%) are next. The factor with the least influence appears to be the size and design and the device (68%).

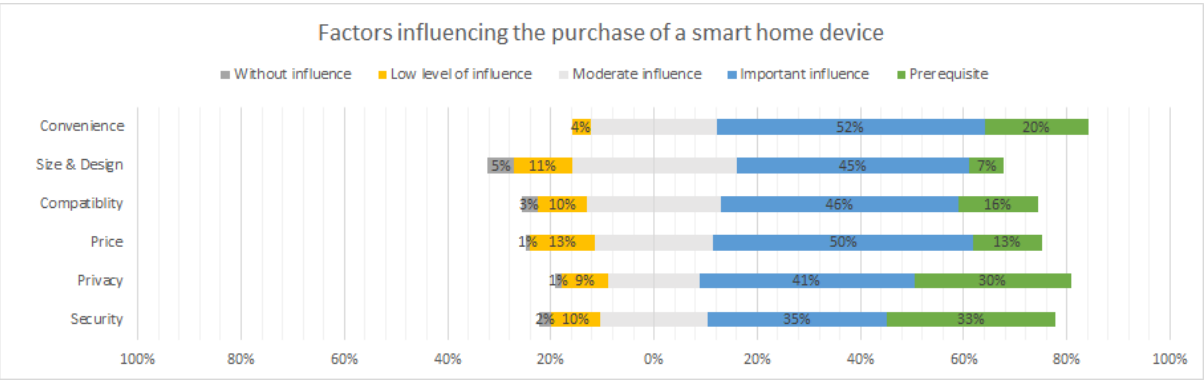


Fig. 9 - Likert plot depicting the factors influencing the purchase of a smart home device of survey respondents.

In an optional question that collected 121 responses, respondents were asked to write down what they saw as the main barriers to adopting a connected home and connected objects in general at this time. From their responses, we noticed that 9 "categories" could be outlined.

Challenge	Occurrence rate in responses
Price	38,84%
Lack of uniform communication standards	20,66%
Privacy	20,66%
Lack of convenience	19,01%
Security	18,18%
Lack of technological knowledge	13,22%
Lack of useful/compelling use cases	9,09%
Internet connection issues	4,13%
Health concerns	3,31%

Table 8 - Current main barriers to the adoption of smart homes and connected objects according to 121 survey respondents.

Please note that some respondents mentioned multiple challenges in their answer which explains a total exceeding 100%. In addition, answers that were mentioned less than three times or that could not be attached to one of the 9 categories are not mentioned in the above table.

As you can see in the table above, it is the price of a connected installation that currently seems to be perceived as the main barrier with an occurrence of 38.84%. Then come the problems of compatibility between objects and the data privacy issues. Lack of convenience and security are also often mentioned by respondents. Some new and interesting elements have also been mentioned such as the lack of knowledge about the technology, how it works

and its various applications which also seems to be an important barrier to the widespread adoption of smart homes and connected devices. The lack of concrete need and the lack of compelling use cases of IoT objects in a home is another challenge, as well as the last two elements: the lack of a sufficiently powerful and stable internet connection and the different health concerns people may have about connected objects (mainly at the “wave production” level). In addition, these results are often confirmed by survey respondents’ level of agreement to statements we exposed them.

Now, let's take a look at the smart home owners sub-category. This category is composed of 49 respondents aged mainly between 25 and 34 years old (36.73%) and living mainly in the United States (53.06%) and Belgium (16,33%). Indeed, 89.66% of respondents living in the United States say they own a smart home. They live in a household composed of 3 or more individuals (57,14%) and have a high income (79,59%). Most of the time, they designed their smart home themselves (95,92%) between 1 and 4 years ago (77,75%). They designed it little by little as a result of the accumulation of many connected objects over time (85,71%).

4.2. Insights drawn from interviews

The interviews we conducted cannot be generalized to a larger population, but nevertheless provided us with interesting information and confirmed a lot of insights we have already been able to draw from our online survey.

First of all, as we have already been able to see from our survey, an interest in new technologies seems to be a prerequisite for the adoption of connected objects in a smart home context. During our interview with a smart homeowner, we found that he has been an early adopter of many different new technologies in the past and has always had a strong appetite for technological innovation. Where, on the contrary, a person who has never experienced a strong technological appeal seems more closed to the idea of adopting connected objects.

A second insight we were able to draw from our interviews is the diverging interest in connected objects depending on the enthusiasm of the interviewee for IoT devices. For a person who has already adopted this technology, the main interest seems to be the increased level of comfort and level of control he can benefit from it coupled with the capacity he has

to remotely manage his home from wherever and whenever he wants. For a person likely to adopt a smart home in the future, the focus seems to be more on automating chores and saving time. Finally, for a person who is not attracted by connected objects, the connected home seems to appear more like an aesthetic gadget with no real added value for the inhabitant.

When talking about the challenges the smart home sector and smart object composing it are currently facing, our interviewees all agree that the price of connected objects is a real obstacle to adoption, as well as the issue of privacy of personal data. For a confirmed user, the main challenge seems to come from the lack of uniformity in the means of inter-object communication, pushing the consumer to carry out long and tedious research to ensure that an object will be able to be integrated with its full potential within the network of objects the users has already built. Finally, for a person who does not wish to adopt this technology, the impact of waves on health is too often underestimated. She explains that when people are working in an urban environment and live in a rural environment, they often have a real desire to disconnect when they return home. She also mentions the growing trend of digital detox shows that people are being fed up with being constantly connected and she believe that this feeling could affect the success of connected homes and connected objects in general. She also adds that for many people, these objects can even induce anxiety.

We have also learned of other factors that could constitute a barrier to the adoption of this technology and that were not mentioned during our online survey. Indeed, for a potential future user, connected objects seem to be too little customizable at the moment and perform their actions under too strict and limited constraints/rules that cannot be modified by the user. According to him the technology does currently not allow objects to be integrated into their user's routine, it is actually the users that currently need to integrate these objects into their routine. That constitutes for him a real brake on adoption and contradicts the idea he has of a connected object that he sees more as a daily helper rather than something he has to adapt to.

Finally, for 2 out of 3 interviewees, what also blocks the growth of connected homes is the lack of a consumer offer with a flagship product/service that brings undeniable added value. According to a connected home owner, people still see the connected home as a toy or gadget

and to have widespread adoption of the technology this vision would need to change and be seen as a real innovation allowing residents to easily and better manage their energy consumption, and increase their comfort and safety.

CHAPTER V – IMPLICATIONS

As the goal of this work is to identify managerial implications that will drive the adoption of IoT-enabled smart homes into households, this part groups the different insights from the literature, our developed user adoption model, the conducted online survey, and the qualitative interviews. Some implications have already been developed in the literature (see Chapter III – Point 3.6), hence those will only be mentioned in this part.

In order to help managers design their interventions, we propose a framework that maps the different types of implications with either internal, external, or customer interactions. It can be observed that implications to these three types have been proposed in this work. It can also be observed that the provided implications are not only technical, but some are also social. This was one of our objectives as it had been observed that the literature mainly focused on the technical aspects of smart homes. Several implications have already been elaborated in the literature. Therefore, we will only refer to them and not elaborate them again in this part. The proposed implications are presented in the following matrix:

			Level of interaction		
			Internal	Interaction with customers	External (other than customer interaction)
Types of implications	Social	Support		X	
		Customer Relationship		X	
		Context understanding			X
		Educate and inform		X	
	Economical	Costs and business model	X		
	Technical	Partnerships			X
		Privacy and Security	X		
		Internal Capabilities	X		
		Design characteristics	X		

Table 9 - Matrix of identified implications, based on type and interaction level

5.1. INTERNAL

5.1.1. COSTS AND BUSINESS MODEL

In the implications identified in the literature, we already noted the need for companies to be ready to adapt their business models. To that regard, several potential considerations were raised: solution-based versus product-based value propositions, horizontal versus vertical diffusion, and industry changes. Solution-based value propositions are based on solutions rather than products. In addition to the previously identified implications, we suggest the following ones:

Companies should take new types of business models into consideration when defining their strategy. Our online survey pointed out that when asked to choose between acquiring a smart home installation through a one-time payment or to rent one on a yearly basis with

device updates and upgrades included (i.e. subscription-based), 36% of the respondents answered the second option. It also appeared that 43% of non-users would opt for the second option. It can be interpreted that non-users rather focus on the provided solution and might also not be ready to make substantial initial investments without knowing what to expect from it. The type of housing contract (i.e. owner versus tenant) might also play a role. We argue that a subscription based business model might be more in line with the more skeptical customers' expectations as it reduces the financial risk associated to an acquisition as well as other costs associated to it such as market research, while providing the convenience of enjoying the latest technologies. Hence, when considering mass market diffusion, the late majority and laggards groups identified by Rogers (2010), that tend to be more skeptical, should also be taken into account. Therefore, companies should not overlook the possibility of implementing alternative business models, such as a subscription-based business models that allow for carefree use, that might be more aligned with some of the innovation adopter groups. This would also allow companies to tap into new revenue sources.

Companies should foster access to smart home by allowing (potential) users to build up their smart home installation over time. The monetary costs were mentioned in our online survey as well as in our interviews to be a high barrier to smart home adoption. In this work, we suggest that a one-time payment of the overall cost of a smart home can be prohibitive for many potential customers. Hence, allowing customers to spread the investment over several years could be beneficial for both companies and customers. A way to do so is by proposing customers to start with an initial basic smart home installation, comprised of the most useful features and devices. This would lower the initial investment required and would allow customers to have a first hands-on experience with the system. As Venkatesh and Bala (2008) suggested, hands-on experience with a system will make users adapt their initial perceptions on the system. Hence, if users have very low self-esteem in their ability to use a smart home system (referred to as 'computer self-efficacy'), are generally afraid or uncomfortable when having to interact with technology ('computer anxiety'), or doubt interacting with a smart home system can be enjoyable ('perceived enjoyment'), they can actually try it out and eventually adjust their initial perceptions on the perceived ease of use of a smart home system. Generally, it is expected that with hands-on experience the perceived ease of use of a system increases, and therefore has an indirect positive effect on

intention to adopt, as highlighted in our research. Hence, the willingness to pay for a smart home can be expected to increase with hands-on experience, which would be a positive outcome for the company. Other positive outcomes can be noted. First, companies would be able to target different price segments based on the sophistication levels, ranging from basic to more advanced installations. Therefore, companies can tap into a larger part of the market. Leaving the possibility to customers to further develop their installation also allows to have customers move from a lower price segment towards a higher price segment, whereas the opposite route is not possible. Second, as it has been mentioned earlier, offering a basic installation could ensure companies to lock customers in, in case they opt for a proprietary system approach. Third, allowing customers to develop their installation over time allows companies to have more interaction with the customers and better engage with them, than it would be the case with a one-time payment. Building an ongoing relationship with customers is key for companies as it allows, amongst other things, to develop the customer's trust in both the company and the technology as well as having more touchpoints with the customer, which can increase future sales. Fourth, as the investments are spread over time, companies generate more stable revenues. Fifth, it also allows new entrants to launch their business with a basic installation, hence lower setup costs, and develop more sophisticated additional devices over time, in comparison to the situation where a complete installation would have to be proposed from day one. Implications for companies include developing installations that are can easily adapt and evolve over time. To that regard, compatibility is considered as key. Companies should also seize the opportunity to build strong and ongoing relationships with the customers, based on trust. Further, companies need to appropriately choose the devices that would be included in the basic installation as these devices should build up users' confidence in the system and push them towards adopting (and purchasing) even more devices. Choosing the right devices customers should start with will mainly depend on the company's value offering, the perceived ease of use and usefulness of the devices, and needs to be aligned to the customers' own requirements and needs.

5.1.2. PRIVACY AND SECURITY

The challenges related to privacy and security have been identified in the literature review. Their potential solutions as well as managerial implications have also been assessed. Therefore, we refer to the "Potential solutions to IoT challenges" in the literature review.

5.1.3. INTERNAL CAPABILITIES

The implications highlighted in the literature review identified some core internal capabilities companies should develop. In that sense, businesses require skills in: product development and marketing, wireless communication, and data management (Saarikko, Westergren & Blomquist, 2017; Lee and Lee, 2015). In addition, other more specific skills in the technologies making part of the IoT framework (e.g. middleware, cloud computing) are also important but might not be as crucial as the ones mentioned earlier (Lee & Lee, 2015).

In addition to that, managers need to decide which competencies will be internalized in the company and which ones will be externalized. While internalizing competencies allows for more control it can be costly and time consuming to build up expertise from scratch. Externalizing some of the competencies can allow to free up more time and resources for the internalized competencies while still achieving top performance by leveraging the recognized expertise of external partners. Externalizing also increases dependence on other companies and therefore it is important to decide on which competencies can and should be externalized.

5.1.4. DESIGN CHARACTERISTICS

Some barriers to adoption of IoT-enabled smart homes can be directly assessed through developing the right design characteristics.

5.1.5. SOCIAL ASPECT

Companies need to better balance the level of smartness and automation of devices with the users' willingness to keep control over the devices. Our survey learned us that people tend to be concerned about loss of control over their environment as well as technology dependence. In addition, one of the persons interviewed emphasized that she was exposed to technologies all day and therefore did not want to be exposed to a connected home when

returning home. Moreover, our model did not provide empirical evidence that perceived controllability had a significant effect on perceived ease of use. Hence, a difference can be made between controllability - that is highly valued by users but does not necessarily improves perceived ease of use - and automation - that replaces human control by machine control and that is therefore supposed to increase objective usability of the smart home. Hence, a distinction can be made between humans being able to better control their devices (e.g. remote controllability at any time and from anywhere) and devices being able to autonomously control themselves, through automation techniques. In other words, the difference between human-to-machine (H2M) interactions and machine-to-machine (M2M) interactions should not be underestimated. Our research leads us to the idea that users are quite reluctant to delegating all of their control and decision-making to computers, as our survey highlights their concerns about loss of control. Developing further, we suggest that users tend to build more negative initial perceptions (i.e. computer anxiety) on M2M than on H2M interactions as they have no direct control over M2M interactions. Indeed, in the first case (i.e. M2M) users become passive while in the second case (i.e. H2M) they remain proactive. Hence, a balance needs to be found between constantly improving smart home devices into 'smart' systems that foster automation, and the human fears of losing control and freedom, as well as their negative initial perceptions on machines as decision-making authority. Therefore, companies should first aim to reduce those negative initial perceptions on M2M control. Secondly, they should find a balance between human control and interaction with the devices and increased automation through more and smarter M2M interactions.

Companies should carefully take into consideration customer needs at the product development stage, not only when selling the products. As it has been highlighted in our model, perceived usefulness and ease of use play a big role in people's intention to adopt a smart home installation. Hence, it is important for managers to take that into consideration early on when developing new products. It may seem obvious but taking into consideration the customers' viewpoint before developing a new product allows to be better aligned with their needs. As a consequence, products that are easier to use and more useful to the customers will tend to have an easier market reach. In contrast, companies that solely focus on the technology (known as 'technology-push' approach) and underestimate the customers'

point of view may effectively develop new and/or better technologies but will find it very difficult to bring those products to the market afterwards. Therefore, the customers' point of view is not only important to take into consideration at the selling stage, but should also be taken into account at the early stages of product development. To put it more bluntly, the selling of the products starts at the product development, not once products reach the warehouse.

5.1.6. TECHNICAL ASPECT

In the literature review, we already identified the need for smart homes to allow for compatibility between devices as it would allow for more flexibility and scalability of the system. The system should also be more adaptable (refer to the literature review for a more elaborated explanation). In this subsection we further draw on these ideas.

Technical development is required in order to foster service reliability. Smart home services' reliability relies on two pillars: the fact that the service should not malfunction, and the accuracy of the service provided. More specifically, the service needs to be sufficiently sophisticated in order to provide services that accurately match the desired outcomes. A system that works but that is not able to accurately anticipate the needs of its users is not perceived as reliable. Hence, technical development is required to make the system more intelligent.

A major barrier to smart home adoption appears to be compatibility between devices from different providers. In order to function properly, a smart home system should allow the different devices constituting the network to communicate with each other in an efficient way. By doing so, the smart home system would be perceived as more flexible as devices could be added and removed more easily and the overall system would adapt to the changing preferences and needs of its users more easily. Hence, the perceived ease of use of the smart home would increase and positively influence users' attitude towards the system, as well as its perceived usefulness. A smart home system that easily integrates other devices also allows users to build up their smart home devices base over time, as they know that new devices will be compatible with their other already acquired devices. A GFTronics employee confessed us (during Batibouw 2020) that it is indeed a common practice for smart home providers to

install a basic smart home system at first, and then propose customers to add other devices and features over time. However, this is usually only applicable to devices from a same provider. Hence, it is also a way for companies to lock customers into their proprietary devices system. This illustrates that companies can have contradictory incentives regarding compatibility between devices from different vendors. It also illustrates that users' optimal welfare (i.e. full compatibility) and companies' optimal welfare do not always overlap. Therefore, managers should carefully weigh the pros and cons associated to full compatibility between devices from different vendors.

Companies should find ways to positively influence the perceived ease of use of the system and, to that regard, designing a user-friendly interface should be a priority. Our model highlighted the importance of a user's perception of ease of use. We believe that system characteristics such as user-friendly interfaces and aesthetically appealing products should have a positive influence on users' perceived enjoyment. Moreover, user friendly interfaces should positively influence the objective usability of the system as well, as the access to the systems' features is enhanced. A more user-friendly interface might as well give the user the perception of having greater control over the system and therefore the users' confidence in his ability to control the system would be fostered. Hence, companies should pay particular attention to ways to enhance perceived ease of use and to that sense designing a user-friendly interface appears to be a priority.

Companies need to make a tradeoff between easy troubleshooting of the system and high level of customization. A challenge that can occur when users interact with the system relates to the expertise and know-how required. Some situations may occur where problems need to be fixed, software needs to be updated, or new devices should be added to the system. In these situations, it is important that companies provide clear and easy to understand guidelines. To that regard, developing a system that is easy to use when facing these situations is important. However, the system's level of complexity should not be too low neither otherwise it more advanced customization of the system might be impossible. Hence, companies have to make a tradeoff between a higher complexity level that allows for more customization and a lower complexity level that allows for easier troubleshooting and updates but that constraints the amount of customization.

5.2. INTERACTION WITH CUSTOMERS

5.2.1. SUPPORT

Service providers need to develop customer trust in order to be perceived as reliable. That is, users need to trust the service providers before they acquire their services. In the smart home context it is no secret that data collection and processing is key for companies to propose more accurate services. With this data-driven approach, security and privacy become a concern for the users. This was highlighted in our survey results where privacy was the third most occurring word in our survey's open question concerning barriers to adoption. Privacy was mentioned as well in one of our interviews. Customers' concerns are exacerbated by the fact that the collected data is directly related to their intimacy (i.e. their home and behaviors). While customers have their private data at stake, companies face 'reputational risk'. In addition, IoT-enabled smart homes allow for more interaction between the devices as well as more remote controllability. This increases the potential damages of security breaches. In addition, Shin, Park and Lee (2018) show that people who care more about personal information tend to postpone smart home appliance purchases. Hence, security and privacy are key concerns and building trust by nurturing relationships with the customers, through more transparency for instance, as well as developing high-level security technologies to prevent data leaks appears to be trivial. We suggest that this will have a positive impact on users' attitude towards adopting smart home services, and indirectly have a strong effect on smart home adoption intention, as our adoption model showed a strong link between attitude and adoption intention. Further, we suggest managers to develop their brand management strategy to build brand trust.

5.2.2. CUSTOMER RELATIONSHIP

It is important for companies to build a relationship with the customers as these might purchase other products to add to their installation. It has already been mentioned that experience plays an important role as users adapt their initial perceptions with hands-on experience. Venkatesh (2000) identified that the perception of external technical support to

use the system (referred to as perception of external control) influenced the perceived ease of use of the system. Therefore, companies should look at ways to provide support. Several ways exist. For instance, online communities may be very useful for companies to keep contact with their customers and help them when they face problems. Customers would value the help, which would have a positive effect on their perception of ease of use. It is also a cheap way for companies to troubleshoot problems as instructions can be given online. In addition, companies can also easily get feedback on their products and track frequent issues that need to be resolved.

5.2.3. EDUCATE AND INFORM

Companies should find ways to have potential customers experience the system. Indeed, we observed some heterogeneity in the responses to our survey of smart home users and non-users. As the main difference between both groups is experience with the system, this suggests that hands-on experience with the system affects users' overall perception of the system. More specifically, experience could be a moderating factor of perceived ease of use and perceived usefulness of a smart home. This has been empirically validated by Venkatesh and Bala (2008) for IT systems. In their work, they provide empirical evidence that experience affects determinants of perceived ease of use (i.e. computer anxiety, computer playfulness, perceived enjoyment, objective usability) as it gives users more information on how easy the system is to use. Then, perceived ease of use positively influences perceived usefulness (Venkatesh et al., 2003) as users value perceived ease of use when forming perceptions about perceived usefulness. With some extrapolation to the smart home context, it can be expected that with hands-on experience users will adjust their initial judgements of perceived ease of use, that are initially based on anchors. Hence, in order to increase perceived ease of use and (indirectly) perceived usefulness of a smart home, that we found to be important determinants of user intention to adopt a smart home, companies should find ways to have potential customers experience the smart home system. For instance, users might have hands-on experience with the system at the company's showroom, or promotional videos might insist on the ease of use of the system.

5.3. EXTERNAL

5.3.1. CONTEXT UNDERSTANDING

Companies need to take into consideration the long replacement cycles of 'traditional' products as well as create more additional value to their products. It can be expected that when targeting mass market adoption, different groups of adopters will adopt the products at a different time (i.e. Rogers' adoption rate) (Rogers, 2010). In the smart home context, we believe that considering smart home products as replacement for traditional products is an important consideration made by some of the (potential) customers. More specifically, we expect adopter groups with longer adoption rates, starting from the early majority group, to highly value the fact that most smart home products are acquired when the traditional products do not function properly anymore. Indeed, while bringing added value, the core functionality of smart home products tends to remain the same as for traditional products. For instance, whether it is remotely controllable or not, a lightning system's core function remains enlightening a space. In addition, we underline the fact that most customers already own a large number of 'traditional' products whose core function is the approximately similar to their IoT-enabled counterparts. Hence, adopter groups who have higher expectations regarding usefulness of smart home devices might want to consider acquisition once their 'traditional' devices are not able to deliver their core functions anymore (e.g. become obsolete, break down). This is in line with our survey observation that showed that 93% of the people who own a smart home built it by acquiring devices over time. It also further supports the compatibility-related implications mentioned earlier. Moreover, it implies that mass market adoption rate will partly depend on the obsolescence rate of those 'traditional' devices and therefore mass-market adoption might take some time. Hence, companies must take it into account when building their long-term strategy as they will need the necessary (financial) resources to survive before mass market adoption. Another implication is that a majority of adopters have low purchase incentives and therefore might develop higher perceived usefulness expectations. Therefore, smart home vendors need to create more additional value, and better inform potential customers about the benefits of a smart home.

Companies should take individual user characteristics into account when designing their products. While this work sets general implications by considering ‘users’ and ‘non users’, it is also important to take into consideration that those individuals have their own characteristics and therefore managers should take that into account when defining interventions to foster user adoption. Amongst the user characteristics that showed different results depending on a specific factor, we can highlight the following factors that companies should take into account: gender, housing contract type (i.e. owner, long term rent, short term rent), age, familiarity with technology. We suggest companies to align the product development with their targeted profile. For instance, when targeting elder people it is important to develop an easy to use and intuitive interface that can be used by people that have limited affinity with technologies. On the contrary, more complex user interfaces including more features for customization can be developed for younger people that are familiar with computers and smartphones.

5.3.2. PARTNERSHIPS

Companies should not only rely on internal capabilities but should also develop partnerships. Some of the competencies should be externalized and finding the right partners then becomes a key asset. Here, information sharing and collaboration are crucial and involve multiple parties and perspectives. Access to those external competencies can be fostered by value networks, ecosystems, or partnerships (Lee & Lee, 2015; Saarikko, Westergren & Blomquist, 2017).

Companies can partner with other companies in order to extend their skill set. Connected products require a broad skill set (broader than for non-connected products) and therefore several parties, with their respective expertise, might work together towards a co-created solution (Burkitt, 2014). Although they are working towards a common goal, each actor also has his own business interest. In that sense, two contradictory business logics exist: vertical diffusion and horizontal diffusion. We refer to the literature review for the elaboration of these two approaches.

CONCLUSION

WORK REVIEW

First, this work provides an extensive review of the literature where a definition is proposed for the main terms related to the IoT-enabled smart home subject (i.e. IoT, smart home, home automation, WSN). Then, as the IoT-enabled smart home is a relatively recent concept that is predicted to develop immensely in the future, the context of its emergence is framed. Further, in order to better grasp the overall situation of the IoT and smart homes domains, a market overview and the enabling technologies are presented. Then, more focused towards the identification of managerial implications, the main challenges and their potential solutions as well as other managerial implications found in the literature are presented. A review of adoption models is also provided in the literature review.

Concerning the research part of this work, in order to identify potential managerial interventions a variety of means were used to collect insights. In order to make sure the identified managerial implications would be aligned with user needs, a user-centered approach was favored. Finally, all the collected insights were put together and presented in a common framework.

CONTRIBUTIONS

First, a plethora of definitions can be found concerning the terms of IoT and smart homes. However, as those terms have a very wide conceptual domain, most works solely focus on the conceptual parts that is of interest to them. It was also noted that some of previous definitions were outdated, mostly because they relied on outdated technological concepts. Since this work focuses on the managerial implications, it required to have a very broad view on these terms that would capture as many of their conceptual dimensions as possible. To do so, different perspectives were taken into account and a review of the most used definitions in previous works was done. We believe that the proposed definitions can be used in future works that require a larger definition of these terms, as it was the case for us.

Second, since this technology binds the fields of IoT and the previous versions of the smart home, we presented both contexts first and identified what we considered as the main reasons for its emergence. To our knowledge, very few articles have tried to identify the main reasons for the emergence of IoT-enabled smart homes specifically. Moreover, most of the articles that did so were written more than five years ago and can therefore be considered as outdated, as the field is evolving at a fast pace.

Third, we provide a market overview where different sources are put together to form a coherent whole. This is not done frequently in the literature as usually authors cite only one specific source. Here, our market overview allows to cross-check different sources and provides a global understanding of the current and predicted future situation.

Fourth, the IoT and smart home fields heavily rely on several enabling technologies. Most of these technologies are still evolving at a very fast pace (e.g. AI, blockchain technology, cloud computing). Hence, it was important to list those enabling technologies and present their state of the art.

Fifth, this work presents a very extensive review of the current challenges faced by the IoT-enabled smart homes. In line with the challenges, it also identifies their respective impacts and the potential solutions that can be undertaken to mitigate those challenges.

Sixth, it was observed that the literature overall lacked research on interventions that could be undertaken by managers to develop the IoT-enabled smart home market. Some of the literature identified barriers and technology-oriented solutions but did not focus on managerial interventions. Moreover, to our knowledge, no extensive review of the literature on potential managerial implications existed. Hence, our work provides (1) a review of the existing literature that was lacking, (2) suggests new managerial interventions, and (3) maps all of these interventions in a framework. This part therefore represents the main contribution of this work to research on managerial implications for IoT-enabled smart homes.

Seventh, a review of existing research on smart home adapted TAM is also provided in the literature review. Several recent works (less than five years old) already proposed an adapted TAM for the smart home application. However, these works mostly used different determinants in their models. Our review of the literature allowed to list and group (when

applicable) the different determinants used (and validated) in past research. Hence, this literature review of the determinants can serve as a base for developing future models.

Eight, another objective of this work was also to provide interventions that would not be too dependent on time or technology. In other words, we believe that most of the provided guidelines are timeless and will not be considered as outdated soon.

LIMITATIONS OF THIS WORK

Several limitations can be highlighted in this work.

First, concerning the data obtained through the online survey. The respondents can be divided into two main groups. A first group of respondents corresponds to people that can directly be related to us (i.e. relatives and relatives of relatives). This group consists of mainly Belgian residents and very few smart home users were observed (i.e. only five). As more answers from smart home users were required, the survey was also shared on several forums related to the smart home field. This corresponds to the second group and nearly all of the respondents were smart home users. They also came from a wide variety of countries, and were English-speaking. Overall, it can be noted that the sample is not homogeneous.

Concerning the adoption model that was developed, several limitations have been observed. First, a relatively high number of indicators have had to be removed from the outer model as they did not match the criteria we initially set. This was quite surprising as most of the questions had been validated in previous research. Since the inner model can only be as reliable as the outer model, we believe that our inner model was partly affected by the low number of indicators remaining. For instance, only one indicator could be used for perceived compatibility. Second, the model appeared to be more reliable when only taking into account the smart home users. This might be explained by users' hands-on experience with the smart home, that provokes users to adjust their initial perceptions about the system. When focusing only on the group of experimented users, these differences between users and non-users are not taken into account anymore. Another explanation might be the fact that all the non-users did not correctly understand what a smart home was. We anticipated this situation by providing definitions for smart home and smart products to mitigate this, but it may not have had the desired impact. Overall, these two reasons prevented us from trying to fit a more

elaborated model, as the lack of reliable indicators and the low sample size prohibited us to add more factors to the model.

Considering the implications that were identified and suggested in this work, it is important to note that while they are aimed for a practical implementation, there are often differences between theory and practice. Moreover, the implications we suggest are not exhaustive, other implications also exist. We also adopted a broad view of the smart home market. In reality, there is a large amount of companies coming from different industries. They all have their particularities, that were not accounted for in this work. Hence, the suggested implications need to be adapted to the company's context and there, it might be that some of these implications will not be relevant. Furthermore, those implications have not been field tested. Additionally, it can be noted that we have not confronted these implications to managers, which we suggest to be done in future research.

FUTURE WORKS

A) SHORT TERM

First of all, we believe that interviews with companies active in the field of connected objects and the smart home sector could prove to be interesting and insightful. Finding out what companies active in these fields are already doing to solve the various challenges of the industry, how they identify their customer target or their vision of the market in the future are all elements that could contribute to the continuation of our work and that could also bring new managerial implications we did not mention. Unfortunately, we were unable to do so, as you'll see in the "personal limitations" section.

Some insights related to user characteristics were developed in this work. However, this work kept a very global scope of users. In future research it would be interesting to further analyze user characteristics and their impact on users' intention to adopt a smart home. This could, for instance, be done by using several user characteristics as moderating factors in the adoption model.

This work provided managerial interventions that were obtained by using a user-centric approach. Indeed, the adoption model studied users' intention to adopt, the survey was

answered by users and potential users, and the qualitative interviews were answered by users and potential users as well. Therefore, we suggest future research to confront the proposed managerial interventions to field practitioners. We believe this can either validate our research or lead to additional insights that would improve the research done in this work.

B) MEDIUM TERM

The adapted TAM model that was used in this work can be enhanced with more factors. For instance, Venkatesh and Bala (2008) identified several determinants of perceived ease of use and perceived usefulness. It would be interesting to observe if those determinants can be adapted or validated in the specific IoT-enabled smart home context.

Further, it should also be looked into alternative models to the TAM as the TAM was initially designed for organizational context, which is very different than the studied context. Hence, the original TAM might be combined with other models (e.g. Value-based Adoption Model) to better explain users' intention to adopt smart homes.

PERSONAL LIMITATIONS

During this work we faced some limitations. First of all, the subject we chose proved to be very technical at times and the lack of standardization in the industry sometimes made our understanding more complicated. Specifically, not being students in IT or computer science, our technical knowledge in areas such as M2M-communication or computer security is limited. A second limitation we have had to face is the global pandemic we are still facing which has somewhat changed our plans. Indeed, we would have liked to conduct interviews with experts in companies active in the field of connected objects for the connected home. To do so, we contacted 7 Belgian companies, but unfortunately, due to the complicated context, we did not manage to get interviews or answers to our questions. Hence, we were not able to confront managers with the implications proposed in this work. Moreover, we hoped to be able to attend events where smart home companies would be represented, which may have allowed to gather insights in a more informal way. Unfortunately, we were able to attend only one gathering of companies (i.e. Batibouw), other events being cancelled.

In addition, one of the objectives of this master thesis being to create a tool to help companies enter and understand the market of IoT-devices for the smart home may be frowned upon by companies that do not want to disclose their strategy or help potential competitors.

REFERENCES

50five.be. (2020). Zigbee vs Z-wave - quelle est la différence ?. Retrieved from https://fr.50five.be/blog/z-wave-ou-zigbee.html

Advanced Mobile Group. (2015). The History of RFID Technology. Retrieved from https://www.advancedmobilegroup.com/blog/the-history-of-rfid-technology

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, 97, 48-65.

Alam, M. R., Reaz, M. B. I., & Ali, M. A. M. (2012). A review of smart homes—Past, present, and future. *IEEE transactions on systems, man, and cybernetics, part C* (applications and reviews), 42(6), 1190-1203.

Ali, B., & Awad, A. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors*, 18(3), 817. doi: 10.3390/s18030817

Ashton, K. (2009). That 'internet of things' thing. *RFID journal*, 22(7), 97-114.

Asimakopoulos, G. and Asimakopoulos, S. (2014), "Understanding switching intention of information systems users", *Industrial Management & Data Systems*, Vol. 114 No. 4, pp. 583-596. https://doi.org/10.1108/IMDS-10-2013-0412

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787-2805. doi: 10.1016/j.comnet.2010.05.010

Balta-Ozkan, N., Boteler, B., & Amerighi, O. (2014). European smart home market development: Public views on technical and economic aspects across the United Kingdom, Germany and Italy. *Energy Research & Social Science*, 3, 65-77.

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy, 63*, 363-374.

Banafa, A. (2018). Secure and smart Internet of Things (IoT): Using Blockchain and AI (1st ed., p. 23). *River Publishers*.

Bell, G., & Kaye, J. (2002). Designing technology for domestic spaces: A Kitchen Manifesto. *Gastronomica*, 2(2), 46-62.

Bloomberg. (2014). The Myo Armband: The Future of Gesture Control [Video]. Retrieved from https://www.youtube.com/watch?v=jOEcsNmTk7g

Brush, A. B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., & Dixon, C. (2011). Home automation in the wild: challenges and opportunities. In *proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2115-2124).

Chan, M., Estève, D., Escriba, C., & Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer methods and programs in biomedicine, 91*(1), 55-81.

Cisco Systems. (2013). Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion. p.2. Retrieved from https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf

Cisco. (2020). What Is Wi-Fi? - Definition and Types. Retrieved from https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html

Cryptomathic. (2020). What is non-repudiation?. Retrieved from https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-non-repudiation

Darby, S. J. (2018). Smart technology in the home: time for more clarity. *Building Research & Information, 46*(1), 140-147.

Davis, F., Bagozzi, R., & Warshaw, P. (1992). Extrinsic and Intrinsic Motivation to Use Computers in the Workplace1. *Journal Of Applied Social Psychology, 22*(14), 1111-1132. doi: 10.1111/j.1559-1816.1992.tb00945.x

De Groote, M., Volt, J., & Bean, F. (2017). Is Europe ready for the smart buildings revolution. *Building Performance Institute Europe* (BPIE).

DeCarlo, M. (2018). Scientific Inquiry in Social Work (pp. 365 - 396).

Demiris, G., Hensel, B. K., Skubic, M., & Rantz, M. (2008). Senior residents' perceived need of and preferences for" smart home" sensor technologies. *International journal of technology assessment in health care, 24*(1), 120.

Dey, S., Roy, A., & Das, S. (2016). Home automation using Internet of Thing. 2016 IEEE 7Th Annual Ubiquitous Computing, *Electronics & Mobile Communication Conference* (UEMCON). doi: 10.1109/uemcon.2016.7777826

Diegel, O., Lomiwes, G., Messom, C., Moir, T., Ryu, H., Thomsen, F., ... & Zhenqing, L. (2005, April). A BLUETOOTH HOME DESIGN@ NZ. *In International Conference on Home-Oriented Informatics and Telematics* (pp. 87-99). Springer, Boston, MA.

Ehrenhard, M., Kijl, B., & Nieuwenhuis, L. (2014). Market adoption barriers of multi-stakeholder technology: Smart homes for the aging population. *Technological forecasting and social change, 89*, 306-315.

Elmasllari, E., & Al-Akkad, A. (2017, May). Smart energy systems in private households: behaviors, needs, expectations, and concerns. In *2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC)* (pp. 152-157). IEEE.

Elprocus. (2020). Basic of RFID System - Types and Working Example of RFID Application. Retrieved from https://www.elprocus.com/rfid-basic-introduction-simple-application/

Engagement Alliance. (2020). What is Gamification. Retrieved from https://engagementalliance.org/what-is-gamification/

Fruhlinger, J. (2018). The Mirai botnet explained: How IoT devices almost brought down the internet. Retrieved from https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Fuhriman, J. (2015). Gamification in Internet of Things Customer Experience | Adobe Blog. Retrieved 3 May 2020, from https://theblog.adobe.com/gamification-in-internet-of-things-customer-experience

Galinina, O., Mikhaylov, K., Andreev, S., Turlikov, A., & Koucheryavy, Y. (2015). Smart home gateway system over Bluetooth low energy with wireless energy transfer capability. EURASIP *Journal on Wireless Communications and Networking, 2015*(1), 178.

Gantz, J., & Reinsel, D. (2011). Extracting value from chaos. IDC Review, 1142(2011), 1-12.

Gartner. (2018). Forecast: IoT Security, Worldwide, 2018.

gdpr-info.eu. (2018). Art. 4 GDPR – Definitions. Retrieved from https://gdpr-info.eu/art-4-gdpr/

Ghayvat, H., Mukhopadhyay, S., Gui, X., & Suryadevara, N. (2015). WSN-and IOT-based smart homes and their extension to smart buildings. *Sensors, 15*(5), 10350-10379.

Ghayvat, H., Mukhopadhyay, S., Liu, J., Babu, A., Elahi, E., & Gui, X. (2015). Internet of Things for smart homes and buildings: Opportunities and Challenges. *Journal Of Telecommunications And The Digital Economy, 3*(4), 33-47. doi: 10.18080/jtde.v3n4.23

GrowthEnabler. (2017). Market pulse report, Internet of Things (IoT) (pp. 14-16). Retrieved from https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems, 29*(7), 1645-1660.

Gunge, V., Yalagi, P. (2016). Smart Home Automation: A literature Review. *International Journal Of Computer Applications* (0975 – 8887), 6-7.

Haller, S., Karnouskos, S., & Schroth, C. (2008, September). The internet of things in an enterprise context. In *Future Internet Symposium* (pp. 14-28). Springer, Berlin, Heidelberg.

Hsu, C., & Lin, J. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers In Human Behavior*, *62*, 516-527. doi: 10.1016/j.chb.2016.04.023

IEEE Standard Computer Dictionary (1990). A Compilation of IEEE Standard Computer Glossaries. *New York: Institute of Electrical and Electronics Engineers*.

Imperva. (2020). What is Social Engineering. Retrieved from https://www.imperva.com/learn/application-security/social-engineering-attack/

Intille, S. S. (2002). Designing a home of the future. IEEE pervasive computing, 1(2), 76-82.

IoT World 2019 : analyse du marché. (2018). Retrieved from https://infodsi.com/articles/177250/iot-world-2019-analyse-du-marche.html

ISO/IEC. (2013). Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) (ISO/IEC Standard No. ISO/IEC 29182-2:2013). Retrieved 14 March 2020, from https://www.iso.org/obp/ui/#iso:std:iso-iec:29182:-2:ed-1:v1:en

Jernigan, S., Ransbotham, S., & Kiron, D. (2016). Data Sharing and Analytics Drive Success With IoT-Creating Business Value With the Internet of Things, Global Executive Study. *MIT Sloan Management Review*.

Kallio, H., Pietilä, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal Of Advanced Nursing, 72*(12), 2954-2965. doi: 10.1111/jan.13031

Kalman, R. (1959). On the general theory of control systems. *IRE Transactions on Automatic Control, 4*(3), 110-110.

Kaspersky. (2020). What Is an Advanced Persistent Threat (APT)?. Retrieved from https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Kastner, W., Neugschwandtner, G., Soucek, S., & Newman, H. M. (2005). Communication systems for building automation and control. *Proceedings of the IEEE, 93*(6), 1178-1203.

Kim, D., & Ammeter, T. (2014). Predicting personal information system adoption using an integrated diffusion model. *Information & Management, 51*(4), 451-464. doi: 10.1016/j.im.2014.02.011

Kim, G., Park, S., & Oh, J. (2008). An examination of factors influencing consumer adoption of short message service (SMS). *Psychology And Marketing, 25*(8), 769-786. doi: 10.1002/mar.20238

Krotov, V. (2017). The Internet of Things and new business opportunities. *Business Horizons, 60*(6), 831-841.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431-440.

Lexico. (2020). Cloud Computing & Big data | Meaning of Cloud Computing & Big data by Lexico. Retrieved from https://www.lexico.com/definition/

Literature Review: Traditional or narrative literature reviews. (2020). Retrieved 1 August 2020, from https://libguides.csu.edu.au/c.php?g=476545&p=3997199#:~:text=A%20narrative%20or%20traditional%20literature,or%20context%20for%20your%20research.

Liu, Y.-Y., Slotine, J.-J. & Barabási, A.-L. (2011). Controllability of complex networks. *Nature*, vol. 473, no. 7346, pp. 167–173.

Luor, T. T., Lu, H. P., Yu, H., & Lu, Y. (2015). Exploring the critical quality attributes and models of smart homes. *Maturitas*, 82(4), 377-386.

Manrique, J. A., Rueda-Rueda, J. S., & Portocarrero, J. M. (2016). Contrasting internet of things and wireless sensor network from a conceptual overview. In *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 252-257). IEEE.

Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change, 138*, 139-154.

Martin, J. (2019). What is access control? A key component of data security. Retrieved from https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html

Maslow, A. H. (1943). A theory of human motivation, *Psychological Review, 50*(4), pp. 370–396.

McClelland, C. (2017). Machine Learning Applications in IoT. Retrieved from https://www.leverege.com/blogpost/machine-learning-applications-in-iot

Membership | Wi-Fi Alliance. (2020). Retrieved from https://www.wi-fi.org/membership

Merriam-Webster. (2020). Biometrics. Merriam-Webster.com dictionary. Retrieved from https://www.merriam-webster.com/dictionary/biometrics

Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative, 1*(1), 1-86.

Miori, V., & Russo, D. (2014). Domotic Evolution towards the IoT. *2014: 28Th International Conference On Advanced Information Networking And Applications Workshops*. p. 811. doi: 10.1109/waina.2014.128

Misra, G. , Kumar, V. , Agarwal, A. , & Agarwal, K. (2016). Internet of Things (IoT) – A Technological Analysis and Survey on Vision, Concepts, Challenges, Innovation Directions, Technologies, and Applications (An Upcoming or Future Generation Computer Communication System Technology). *American Journal of Electrical and Electronic Engineering, 4*(1), 23-32.

Mohammed, A., Seeam, A., Bellekens, X., Nieradzinska, K., & Ramsurrun, V. (2016). Gesture based IoT light control for smart clothing. *2016 IEEE International Conference On Emerging Technologies And Innovative Business Practices For The Transformation Of Societies (Emergitech)*. doi: 10.1109/emergitech.2016.7737326

Monostori, L. (2018). Cyber-Physical Systems. *CIRP Encyclopedia Of Production Engineering*, 1-8. doi: 10.1007/978-3-642-35950-7_16790-1

Morris, M. E., Adair, B., Miller, K., Ozanne, E., Hansen, R., Pearce, A. J., & Said, C. M. (2013). Smart-home technologies to assist older people to live well at home. *Journal of aging science, 1*(1), 1-9.

Myo Team. (2018). Getting started with your Myo armband. Retrieved from https://support.getmyo.com/hc/en-us/articles/203398347-Getting-started-with-your-Myo-armband

Norton. What Is A Botnet?. Retrieved from https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

Noura, M., Atiquzzaman, M. & Gaedke, M. (2019). Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mobile Netw Appl 24*, 796–809. doi: 10.1007/s11036-018-1089-9

Onwuegbuzie, A., & Frels, R. (2016). 7 steps to comprehensive literature review (pp. 24-25). London: SAGE.

Oracle. (2015). Energize Your Business with IoT Enabled Applications. Retrieved from https://www.oracle.com/assets/oracle-iot-cloud-service-2625351.pdf

Oreg, S. (2006). Personality, context, and resistance to organizational change. European *Journal of Work and Organizational Psychology*, 15(1), 73–101.

Park, E., Baek, S., Ohm, J., & Chang, H. (2014). Determinants of player acceptance of mobile social network games: An application of extended technology acceptance model. *Telematics And Informatics, 31*(1), 3-15. doi: 10.1016/j.tele.2013.07.001

Pauvres, moyens et riches ? Les revenus par type de ménage. (2020). Retrieved 6 March 2020, from http://www.observationsociete.fr/categories-sociales/donneesgenerales/riches-pauvres-moyens.html

Pirbhulal, S., Zhang, H., E Alahi, M., Ghayvat, H., Mukhopadhyay, S., Zhang, Y., & Wu, W. (2016). A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network. *Sensors, 17*(12), 69. doi: 10.3390/s17010069

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard business review, 92*(11), 64-88.

Porter, M. E., & Heppelmann, J. E. (2015). How smart, connected products are transforming companies. *Harvard business review, 93(*10), 96-114.

Privacy Impact Assessment. (2018). Retrieved 4 August 2020, from https://gdpr-info.eu/issues/privacy-impact-assessment/

Qualcomm Technologies, Inc. (2016). Wireless Connectivity for Advanced Outdoor Lighting Systems. Retrieved from https://www.energy.gov/sites/prod/files/2016/06/f32/koenig_comm-fndmntls_cls2016.pdf

Ram, S. (1987). A model of innovation resistance. *Advances in Consumer Research, 14*(1), 208–212.

Ray, B. (2015). Bluetooth Vs. Bluetooth Low Energy (BLE): What's The Difference?. Retieved 10 March 2020, from https://www.link-labs.com/blog/bluetooth-vs-bluetooth-low-energy

Reinisch, C., Kofler, M., Iglesias, F., & Kastner, W. (2011). Thinkhome energy efficiency in future smart homes. *EURASIP Journal on Embedded Systems, 2011*(1), 104617.

Reinsel, D., Gantz, J., & Rydning, J. (2018). Data age 2025: the digitization of the world from edge to core. *IDC White Paper Doc# US44413318*, 1-29.

Ritholtz, B. (2018). Millennials Are Out of the Basement and Into Buying Homes. Retrieved from https://www.bloomberg.com/opinion/articles/2018-02-02/millennials-are-out-of-the-basement-and-into-buying-homes

Roduner, C., Langheinrich, M., Floerkemeier, C., & Schwarzentrub, B. (2007, May). Operating appliances with mobile phones–strengths and limits of a universal interaction device. In *International Conference on Pervasive Computing (pp. 198-215).* Springer, Berlin, Heidelberg.

Rouse, M. (2016). Internet of things (IoT). *IoT Agenda*.

Saarikko, T., Westergren, U. H., & Blomquist, T. (2017). The Internet of Things: Are you ready for what's coming?. *Business Horizons, 60*(5), 667-676.

Samuel, S. (2016). A review of connectivity challenges in IoT-smart home. *2016 3Rd MEC International Conference On Big Data And Smart City (ICBDSC)*. doi: 10.1109/icbdsc.2016.7460395

Sarma, A. C., & Girão, J. (2009). Identities in the future internet of things. *Wireless personal communications, 49*(3), 353-363.

Schurgot, M., Shinberg, D., & Greenwald, L. (2015). Experiments with security and privacy in IoT networks. *2015 IEEE 16Th International Symposium On A World Of Wireless, Mobile And Multimedia Networks (Wowmom)*. doi: 10.1109/wowmom.2015.7158207

Serrenho, T., Bertoldi, P., Smart home and appliances: State of the art - Energy, Communications, Protocols, Standards, EUR 29750 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-03657-9, doi:10.2760/453301, JRC113988.

Shin, D. (2009). Determinants of customer acceptance of multi-service network: An implication for IP-based technologies. *Information & Management, 46*(1), 16-22. doi: 10.1016/j.im.2008.05.004

Smith, B., & Linden, G. (2017). Two Decades of Recommender Systems at Amazon.com. *IEEE Internet Computing, 21*(3), 12-18. doi: 10.1109/mic.2017.72

Stanislav, M., & Lanier, Z. (2020). DEF CON 22 - Mark Stanislav & Zach Lanier - The Internet of Fails - Where IoT Has Gone Wrong [Video]. Retrieved from https://www.youtube.com/watch?v=WHdU4LutBGU&fbclid=IwAR3eZwD7ROtKMNsatiBMXBBnAI-xWmrek3KPgC4ByGOf_-ulz807KNhLttA

Statista. (2019). Smart Home Report 2019. Retrieved from https://www.statista.com/outlook/283/100/smart-home/worldwide

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

Tanwar, S., Patel, P., Patel, K., Tyagi, S., Kumar, N., & Obaidat, M. S. (2017, July). An advanced internet of thing based security alert system for smart home. In *2017 International Conference on Computer, Information and Telecommunication Systems (CITS)* (pp. 25-29). IEEE.

Tierney, A. (2016). Thermostat Ransomware: a lesson in IoT security | Pen Test Partners. Retrieved from https://www.pentestpartners.com/security-blog/thermostat-ransomware-a-lesson-in-iot-security/

Truong, N., Jayasinghe, U., Um, T., & Myoung Lee, G. (2016). A Survey on Trust Computation in the Internet of Things. p.2.

Tsai, H., Chien, J-L., and Tsai M. (2014). The influence of systems usability and user satisfaction on continued internet banking services usage intention: empirical evidence from Taïwan. *Electronic Commerce Research, vol 14*, no. 2., pp 137-169.

Ungureanu, H. (2016). Massive Dyn DDOS Attack: Experts Blame Smart Fridges, DVRs And Other IoT Devices Why Your Internet Went Down. Retrieved from https://www.techtimes.com/articles/183339/20161024/massive-dyn-ddos-attack-experts-blame-smart-fridges-dvrs-and-other-iot-devices-why-your-internet-went-down.htm

van Dijk, A., & Teuben, H. (2015). Smart Cities: How rapid advances in technology are reshaping our economy and society. Deloitte. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/deloitte-nl-ps-smart-cities-report.pdf

van Kranenburg, R., & Bassi, A. (2012). IoT Challenges. *Communications In Mobile Computing, 1*(1). doi: 10.1186/2192-1121-1-9

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27*(3), 425. doi: 10.2307/30036540

Verma, A. (2018). The Relationship between IoT, Big Data, and Cloud Computing. Retrieved from https://www.whizlabs.com/blog/relationship-between-iot-big-data-cloud-computing/

Wang, M. M., Cao, J. N., Li, J., & Dasi, S. K. (2008). Middleware for wireless sensor networks: A survey. *Journal of computer science and technology, 23*(3), 305-326.

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. Business Horizons, 58(6), 615-624.

What is TLS & How Does it Work?. (2020). Retrieved 4 August 2020, from https://www.internetsociety.org/deploy360/tls/basics/#:~:text=TLS%20Basics,card%20numbers%2C%20and%20personal%20correspondence

Wi-Fi Alliance. (2020). Certification Process Overview (pp. 8-14). Retrieved from https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Alliance_Certification_Process_Overview_v3.5_1.pdf

Wi-Fi HaLow | Wi-Fi Alliance. (2020). Low power, long range Wi-Fi for IoT. Retrieved from https://www.wi-fi.org/discover-wi-fi/wi-fi-halow

Wurm, J., Hoang, K., Arias, O., Sadeghi, A., & Jin, Y. (2016). Security analysis on consumer and industrial IoT devices. *2016 21St Asia And South Pacific Design Automation Conference (ASP-DAC)*. doi: 10.1109/aspdac.2016.7428064

Z-Wave Alliance. (2012). Z-Wave Alliance Announces 700th Certified Product - Z-Wave Alliance. Retrieved from https://z-wavealliance.org/z-wave-alliance-announces-700th-certified-product/

Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014, November). IoT security: ongoing challenges and research opportunities. *In 2014 IEEE 7th international conference on service-oriented computing and applications* (pp. 230-234). IEEE.

Zigbee - Zigbee Alliance. (2020). Zigbee. Retrieved from https://zigbeealliance.org/solution/zigbee/

APPENDICES

APPENDIX 1 - ONLINE SURVEY QUESTIONNAIRE

Link	**Question Number**	**Question asked**	**Possible answers**
Moderator Variable	Q1	EN: Please select your age group FR: Veuillez sélectionner la tranche d'âge vous correspondant	18 - 24 25 - 34 35 - 44 45 - 54 55 - 64 65+
Moderator Variable	Q2	EN: Gender FR: Identité de genre	Male Female Do not wish to communicate Other

Moderator Variable	Q3	EN: Where do you live? FR: Dans quel pays résidez-vous?	List of countries
Moderator Variable	Q4	EN: Please select your monthly income level FR: Veuillez sélectionner votre niveau de revenu mensuel	0€ - 1.270€ (0 USD - 1 471 USD) 1.271€ - 2.297€ (1 472 USD - 2 661 USD) 2298€ or more (2 662 USD or more)
Moderator Variable	Q5	EN: How many smart home devices do you own? FR: Combien d'objets connectés possédez au sein de votre habitation?	None Between 1 to 5 5 or more
Moderator Variable	Q6	EN: Out of how many members is your household composed? FR: Combien d'individus composent votre ménage?	Two or less Three or more
Moderator Variable	Q7	EN: What type of residence do you live in? FR: Quel est votre type d'habitation?	Apartment House

Moderator Variable	Q8	EN: Where do you live? FR: Comment décririez-vous votre environnement?	Urban area Rural area
Moderator Variable	Q9	EN: What type of contract do you have? FR: Quel type de contrat avez-vous pour votre logement?	Rent for less than five years Rent for five years or more I am the owner
Moderator Variable	Q10	EN: Are you interested in one of the following topics: new technologies, home security, home energy use, assisted living and environment? FR: Portez-vous un intérêt pour l'un des sujets suivants: nouvelles technologies, sécurité de la maison, consommation énergétique de la maison, logement assisté et environnement?	Yes No

Actual Use	Q11	EN: Do you own a smart home installation? FR: Êtes-vous propriétaire d'une habitation intelligente ('smart home')?	Yes No

Questions asked to smart homeowners only:

Link	**Question**	**Question asked**	**Possible answers**

	Number		
Moderator	Q12O	EN: At what occasion did you build a smart home? FR: À quelle occasion avez-vous conçu votre habitation intelligente?	Built it up by acquiring smart devices over time When building the house or moving in When renovating / modernizing the home
Moderator	Q13O	EN: Did you develop the smart home installation by yourself? FR: L'avez-vous conçue vous-même?	Yes No
Moderator	Q14O	EN: How many years ago was the smart home developed? FR: Depuis combien d'années l'avez-vous conçue?	Number
Perceived enjoyment (Kim, Park & Choi, 2017)	Q15O	EN: Using smart appliances in a home is enjoyable and fun FR: Utiliser des objets connectés dans une maison est agréable et amusant	Strongly disagree Disagree Neutral Agree
Perceived connectedness	Q16O	EN: Connecting smart home devices from different vendors does not create problems	

(Yang, Lee & Lee, 2018)		FR: Connecter des objets connectés de différents vendeurs ne crée pas de problèmes	Strongly agree
Perception of control	Q17O	EN: Using a smart home system makes me feel dependent on technology FR: Je me sens dépendent des technologies lorsque j'utilise un objet connecté	
Perceived costs (Park, Han & Kwon, 2017)	Q18O	EN: Building a smart home environment is expensive overall FR: Dans l'ensemble, c'est coûteux d'acquérir une habitation intelligente	
Perceived cost (Park, Han & Kwon, 2017)	Q19O	EN: Installing and operating IoT technologies in a smart home environment are a burden to me FR: Installer et utiliser des objets connectés est un fardeau pour moi	
Perceived value	Q20O	EN: The value created by a smart home outweighs its costs (monetary and non-monetary) FR: La valeur ajoutée d'une habitation intelligente surclassent ses coûts (monétaires et non monétaires)	
Perceived usefulness	Q21O	EN: Smart home devices make my life more comfortable FR: Les objets connectés me rendent la vie plus confortable	

(Kim, Park & Choi, 2017)			
Perceived usefulness (Kim, Park & Choi, 2017)	Q22O	EN: I believe a smart home environment is useful to my lifestyle FR: Je pense qu'une habitation intelligente est utile pour mon style de vie	
Perceived complexity (Kim, Park & Choi, 2017)	Q23O	EN: A smart home environment is not complex FR: Une habitation intelligente n'a rien de complexe	
Intention to use (Park, Han & Kwon, 2017)	Q24O	EN: I recommend others to use IoT technologies in a smart home environment FR: Je recommande d'autres personnes d'acquérir une maison intelligente	
Perceived automation	Q25O	EN: Smart home devices help the residents proactively without human intervention FR: Une habitation intelligente supporte ses habitants de manière proactive et sans intervention humaine	

The following questions were asked to all respondents:

Link	**Question Number**	**Question asked**	**Possible answers**
Adoption intention (Yang, Lee & Lee, 2018)	Q26	EN: In the future, would you be willing to purchase a smart home? FR: Dans le futur, seriez-vous prêt à acquérir une maison connectée?	Yes No
Business Model	Q27	EN: If you were to choose, you would prefer to: A - Proceed to a one-time payment for a smart home and fully own all of the devices. Acquérir une installation d'habitation intelligente (de manière définitive) B - Take a yearly subscription from a provider, that includes product upgrades, updates and maintenance. FR: A - Acquérir une installation d'habitation intelligente (de manière définitive) B - Souscrire à un abonnement annuel pour sa location, incluant les mises à jour des services et produits	Option A Option B

	Q28	EN: Would you be willing to invest more for a smart home than a traditional one? FR: Seriez-vous prêt à investir plus pour une maison connectée qu'une maison traditionnelle?	Yes No
	Q29	EN: If the answer to the previous question is yes, what percentage of your purchase budget could you afford to pay extra to have your home connected. (I am willing to buy a house for X€ and I am willing to invest Y% more so that it is connected) FR: En cas de réponse positive à la question précédente, quel pourcentage de votre budget d'achat pourriez-vous payer en plus afin que votre maison soit connectée. (je suis prêt(e) à acheter une maison à X€ et je suis prêt(e) à investir Y% en plus afin qu'elle soit connectée)	Less than 1% Between 1 and 5% Between 5 and 10% More than 10%
	Q30	EN: Smart appliances (vacuum cleaners, fridge, ...) FR: Appareils ménagers (aspirateurs, frigo, ...)	No interest Low interest Moderate interest Interested Very interested
	Q31	EN: Home control devices (thermostat) FR : Appareils de contrôle de l'habitation (thermostat)	
	Q32	EN: Security devices (security camera, alarms,...) FR: Sécurité (alarmes, caméras,...)	
	Q33	EN: Home entertainment	

		FR: Divertissement	
	Q34	EN: Lighting & Comfort FR: Confort et éclairage	
	Q35	EN: Energy Management FR : Gestion énergétique	

Security	Q36	EN: Security (hacking) FR: Securité (piratage)	Without influence Low influence Moderate influence important influence prerequisite
Privacy	Q37	EN: Privacy FR : Vie privée	
Perceived cost, Perceived fee	Q38	EN: Price FR: Prix	
(Inter)connectedness Compatibility	Q39	EN: Compatibility between different smart objects FR: Compatibilité entre différents objets	

Usefulness	Q40	EN: Convenience FR : Facilité d'utilisation	
Fit (aesthetic)	Q41	EN: Size and design of the smart device FR: Taille et design de l'objet	

Perceived enjoyment (Park, Han & Kwon, 2017)	Q42	EN: I think using IoT technologies in a smart home environment is a nice idea FR: Utiliser des objets connectés est une bonne idée	Strongly disagree Disagree Neutral Agree Strongly agree
Attitude (Park, Han & Kwon, 2017)	Q43	EN: I have positive feelings toward IoT technologies in a smart home environment FR: J'ai un sentiment positif à l'égard de l'utilisation d'objets connectés	
Adaptability /Flexibility	Q44	EN: It should be easy to add new devices to the smart home system (without much effort) FR: Cela devrait être facile d'ajouter des objets à son installation intelligente	
Fit (conceptual)	Q45	EN: I am ready to slightly adapt my routine to match with the smart home's working	

		FR: Je suis prêt à faire des efforts pour adapter mon quotidien au fonctionnement de l'installation intelligente
Fit (conceptual)	Q46	EN: I am ready to substantially adapt my routine to match the smart home's working FR: Je suis prêt à faire des efforts considérables pour adapter mon quotidien au fonctionnement de l'installation intelligente
Privacy protection (Kim, Park & Choi, 2017)	Q47	EN: I am concerned about how my personal information is/would be managed FR: Je me sens concerné par la gestion de mes données personnelles
Future use intention (Kim, Park & Choi, 2017)	Q48	EN: I intend to use smart home services in the future FR: J'ai l'intention d'utiliser des objets connectés à l'avenir
Reliability (Yang, Lee & Lee, 2018)	Q49	EN: I believe smart home service providers are reliable FR: Je pense que les prestataires de services d'une habitation intelligente sont fiables

Interoperability / compatibility	Q50	EN: Connecting different devices with each other FR: Connecter différents objets ensemble	Not important Less important Indifferent (50-50) Important Very important
Compatibility (Park, Han & Kwon, 2017)	Q51	EN: Smart devices are compatible with my other devices and services FR: Les objets connectés doivent être compatibles avec mes autres objets et services souscrits	
Perceived control controllability usability	Q52	EN: Controlling smart home appliances simply and easily FR: Connecter les objets connectables de façon simple et facile	
Remote control (Yang, Lee & Lee, 2018)	Q53	EN: Controlling smart home services anywhere FR: Contrôler des objets de n'importe où	
Remote control (Yang, Lee & Lee, 2018)	Q54	EN: Controlling smart home services anytime FR: Contrôler des objets à n'importe quel moment	

Link	Question Number	Question asked	Possible answers
	Q55	EN: What do you see as the main barriers to the widespread adoption of connected objects within the home environment and connected homes more generally? FR: Selon vous, quels sont les principaux obstacles à l'adoption généralisée des objets connectés au sein de l'habitation et, de manière plus générale, des maisons connectées?	Open
	Q56	EN: Do you know any Belgian companies active in the field of connected objects or connected home? If yes, which one(s)? FR: Connaissez-vous des entreprises Belges actives dans le milieu des objets connectés ou de la maison connectée? Si oui, la(les)quelle(s)?	Open

APPENDIX 2 – INTERVIEW GUIDE

Smart Home Interview Guide: Main topics to be covered

0. Definition of IoT-enabled devices and Smart Home

1. Personal information
   a) Please present yourself to us
   b) Present your household

2. Interest in new technologies
   a) Describe your interest in new technologies
   b) Describe your relationship to new technologies

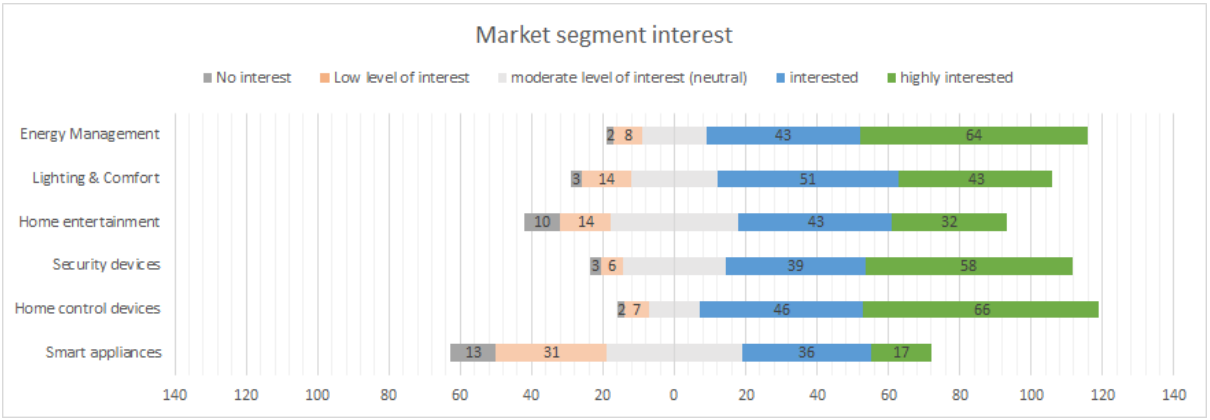
3. Smart Home and connected devices
   a) Describe your relationship to smart IoT devices and Home automation
   b) What activities would you be willing to automate in your home?
   c) From your view what might these smart devices bring to you and your home? What makes people adopt them?

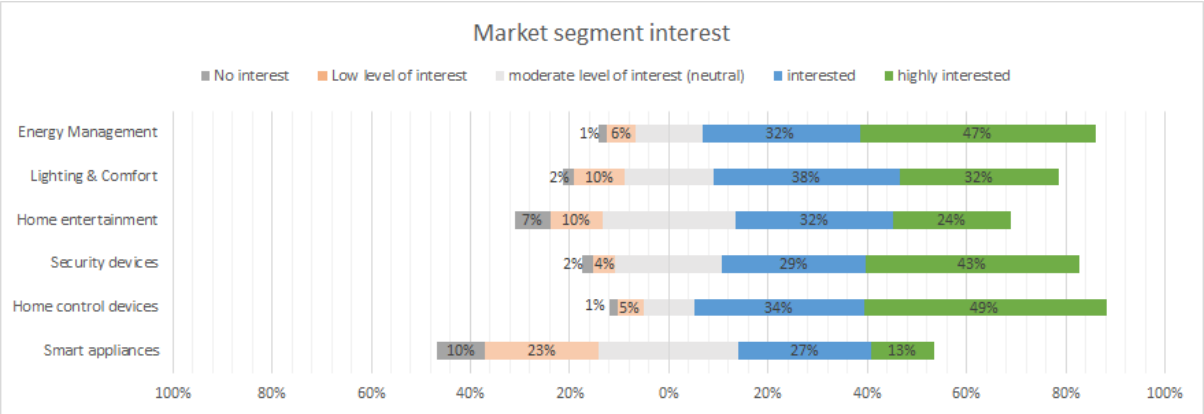
4. Challenges faced by the industry
   a) According to you, what are the main barrier to mass adoption of smart home technologies?
   b) What functionality do you think would make this technology even more popular?

5. Remarks

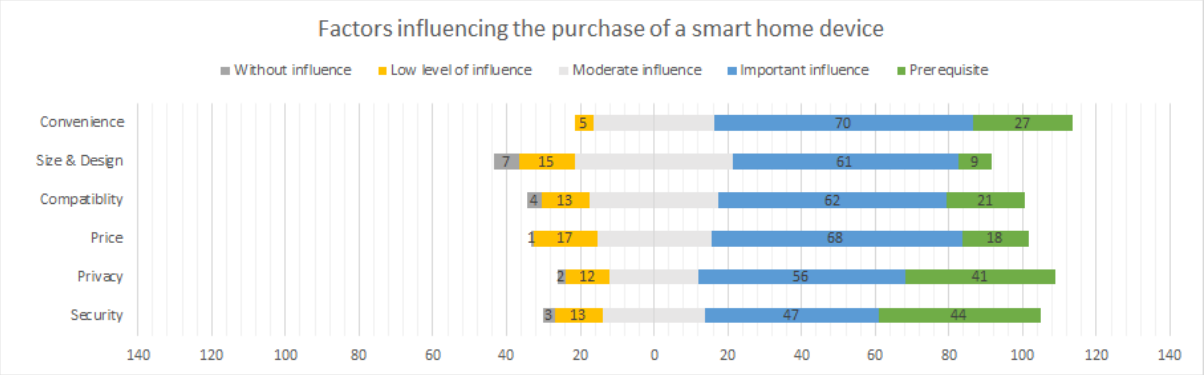
APPENDIX 3 - LIKERT PLOTS DERIVED FROM ONLINE SURVEY RESPONSES

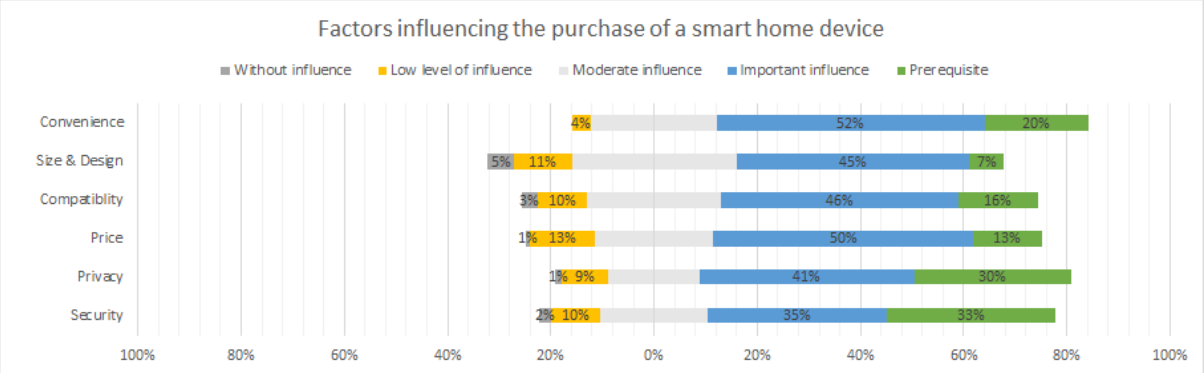
1.



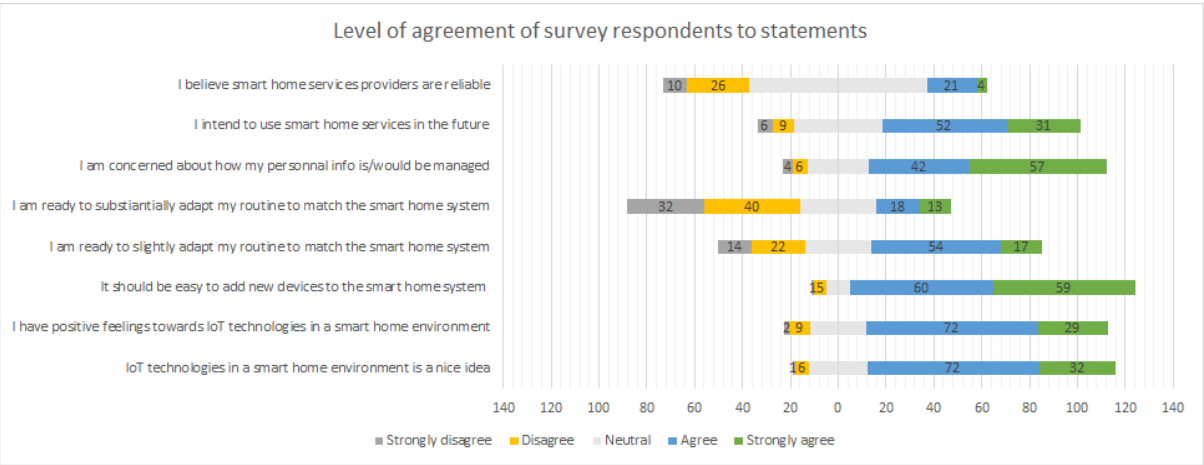


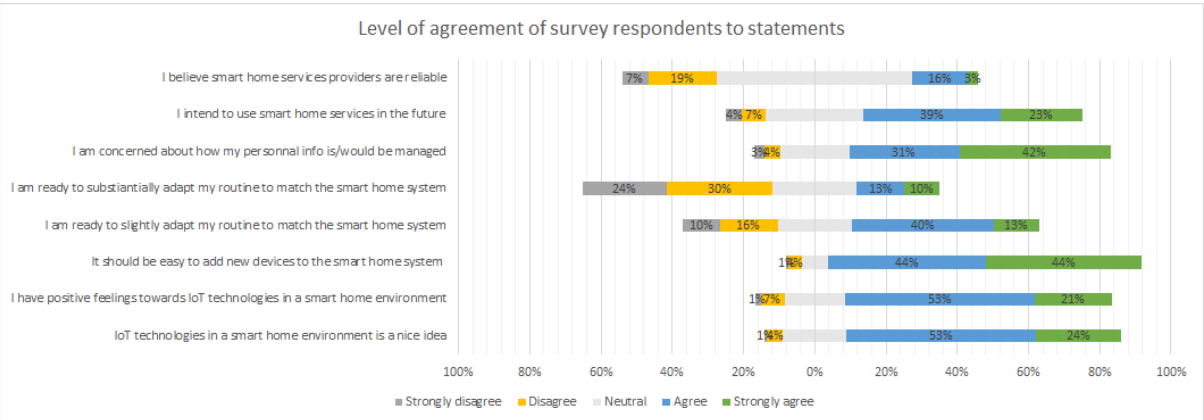
2.


Factors influencing the purchase of a smart home device
Without influence
Low level of influence
Moderate influence
Important influence
Prerequisite
Convenience
Size & Design
Compatiblity
Price
Privacy
Security
5
70
27
7
15
61
9
4
13
62
21
1
17
68
18
2
12
56
41
3
13
47
44
140
120
100
80
60
40
20
0
20
40
60
80
100
120
140

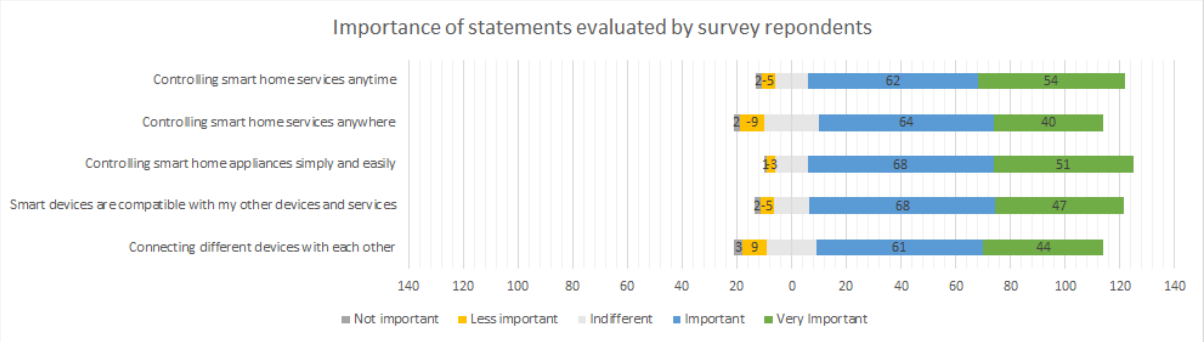

Factors influencing the purchase of a smart home device
Without influence
Low level of influence
Moderate influence
Important influence
Prerequisite
Convenience
Size & Design
Compatiblity
Price
Privacy
Security
4%
52%
20%
5%
11%
45%
7%
3%
10%
46%
16%
1%
13%
50%
13%
1%
9%
41%
30%
2%
10%
35%
33%
100%
80%
60%
40%
20%
0%
20%
40%
60%
80%
100%

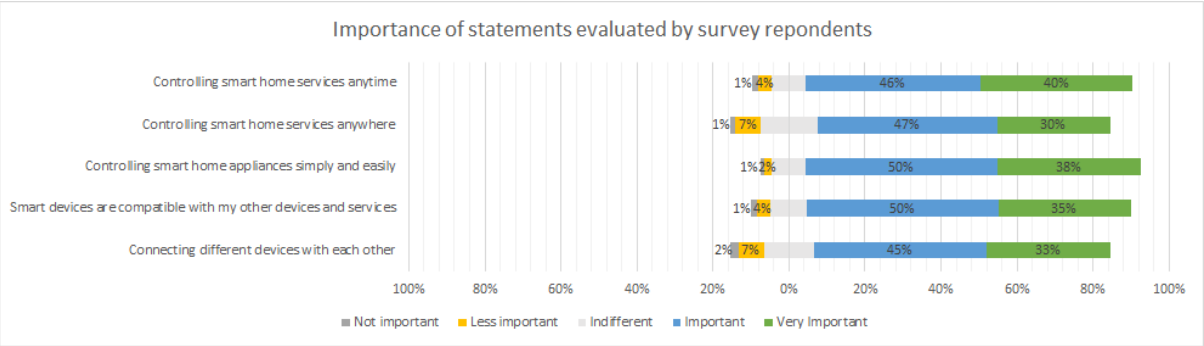
3.


Level of agreement of survey respondents to statements
I believe smart home services providers are reliable
I intend to use smart home services in the future
I am concerned about how my personnal info is/would be managed
I am ready to substiantially adapt my routine to match the smart home system
I am ready to slightly adapt my routine to match the smart home system
It should be easy to add new devices to the smart home system
I have positive feelings towards IoT technologies in a smart home environment
IoT technologies in a smart home environment is a nice idea
10
26
21
4
6
9
52
31
4
6
42
57
32
40
18
13
14
22
54
17
15
60
59
2
9
72
29
1
6
72
32
140
120
100
80
60
40
20
0
20
40
60
80
100
120
140
Strongly disagree
Disagree
Neutral
Agree
Strongly agree

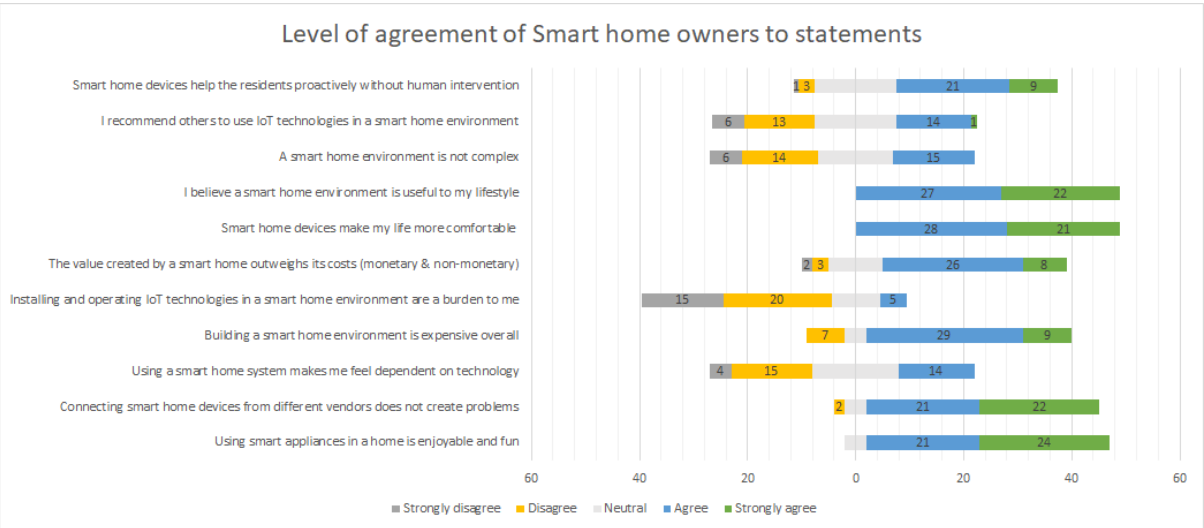

Level of agreement of survey respondents to statements
I believe smart home services providers are reliable
I intend to use smart home services in the future
I am concerned about how my personnal info is/would be managed
I am ready to substiantially adapt my routine to match the smart home system
I am ready to slightly adapt my routine to match the smart home system
It should be easy to add new devices to the smart home system
I have positive feelings towards IoT technologies in a smart home environment
IoT technologies in a smart home environment is a nice idea
7%
19%
16%
3%
4%
7%
39%
23%
3%
8%
31%
42%
24%
30%
13%
10%
10%
16%
40%
13%
1%
44%
44%
1%
7%
53%
21%
1%
4%
53%
24%
100%
80%
60%
40%
20%
0%
20%
40%
60%
80%
100%
Strongly disagree
Disagree
Neutral
Agree
Strongly agree

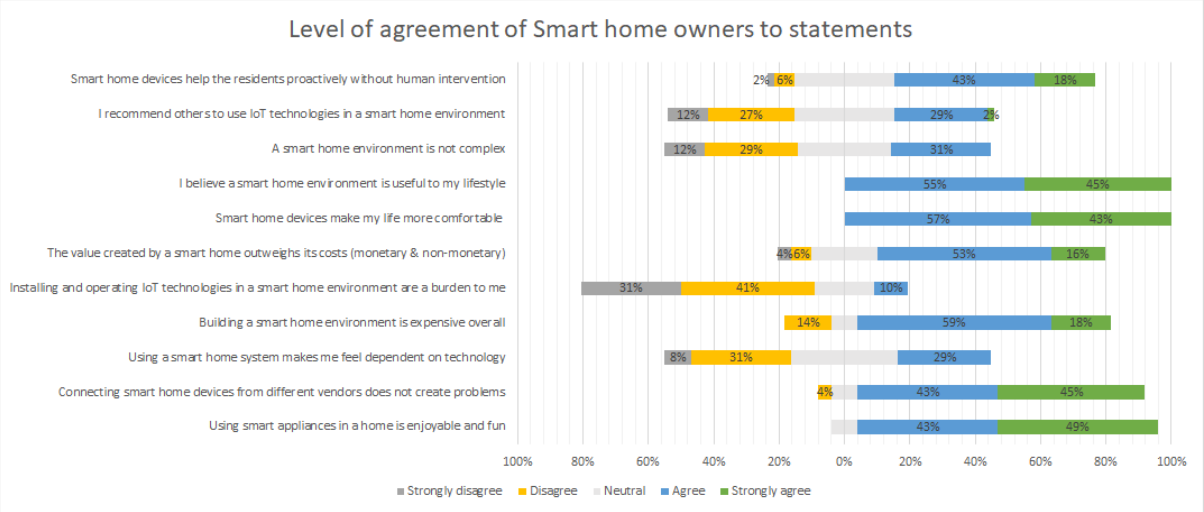
4.


Importance of statements evaluated by survey repondents
Controlling smart home services anytime
Controlling smart home services anywhere
Controlling smart home appliances simply and easily
Smart devices are compatible with my other devices and services
Connecting different devices with each other
2 5 62 54
2 9 64 40
1 3 68 51
2 5 68 47
3 9 61 44
140 120 100 80 60 40 20 0 20 40 60 80 100 120 140
Not important
Less important
Indifferent
Important
Very Important


Importance of statements evaluated by survey repondents
Controlling smart home services anytime
Controlling smart home services anywhere
Controlling smart home appliances simply and easily
Smart devices are compatible with my other devices and services
Connecting different devices with each other
1% 4% 46% 40%
1% 7% 47% 30%
1% 2% 50% 38%
1% 4% 50% 35%
2% 7% 45% 33%
100% 80% 60% 40% 20% 0% 20% 40% 60% 80% 100%
Not important
Less important
Indifferent
Important
Very Important

5.


Level of agreement of Smart home owners to statements
Smart home devices help the residents proactively without human intervention
I recommend others to use IoT technologies in a smart home environment
A smart home environment is not complex
I believe a smart home environment is useful to my lifestyle
Smart home devices make my life more comfortable
The value created by a smart home outweighs its costs (monetary & non-monetary)
Installing and operating IoT technologies in a smart home environment are a burden to me
Building a smart home environment is expensive overall
Using a smart home system makes me feel dependent on technology
Connecting smart home devices from different vendors does not create problems
Using smart appliances in a home is enjoyable and fun
1 3 21 9
6 13 14 1
6 14 15
27 22
28 21
2 3 26 8
15 20 5
7 29 9
4 15 14
2 21 22
21 24
60 40 20 0 20 40 60
Strongly disagree
Disagree
Neutral
Agree
Strongly agree



APPENDIX 4 - OUTER MODEL EVALUATION STATISTICS

- Cronbach's alpha and Rho_A

	Cronbach's Alpha	rho_A
Attitude	0.341	0.392
Intention to Adopt	0.577	0.587
Perceived Compatibility	1.000	1.000
Perceived Ease of Use	0.268	0.279
Perceived Enjoyment	0.453	0.503
Perceived Usefulness	0.885	0.896
Perceived controllability	0.669	0.830

Sacrifices		1.000

- Fornell and Larker Criterion - Discriminant Validity Test

	Attitude	Intention to Adopt	Perceived Compatibility	Perceived Ease of Use	Perceived Enjoyment	Perceived Usefulness	Perceived controllability	Sacrifices
Attitude	0.771							
Intention to Adopt	0.456	0.838						
Perceived Compatibility	-0.014	-0.098	1.000					
Perceived Ease of Use	0.483	0.324	-0.031	0.759				
Perceived Enjoyment	0.630	0.314	0.097	0.382	0.800			
Perceived Usefulness	0.290	0.357	-0.008	0.494	0.336	0.947		
Perceived controllability	0.226	0.224	-0.052	0.163	0.212	0.141	0.859	
Sacrifices	0.119	-0.181	0.237	0.147	0.141	0.131	0.013	

- VIF Values

	VIF
Q21: comfortable	2.701

Q22: usefulToLifestyle	2.701
Q53: controlAnywhere	1.338
Q54: controlAnytime	1.338
Q19: burden	1.309
Q18: PerceivedFee	1.263
Q24: reccommend	1.197
Q48: FutureIntentionToUse	1.197
Q17: Apathy, LossOfControl	1.106
Q42: niceIdea	1.094
Q15: PerceivedEnjoyment	1.094
Q47: concernedPersonalInfo	1.066
Q45: slightlyAdaptRoutine	1.044
Q43: positiveFeelings	1.044
Q25: perceivedAutomation, woHumanIntervention	1.025
Q44: shouldBeEasy	1.025
Q16: Compatibility	1.000

APPENDIX 5 - INNER MODEL EVALUATION STATISTICS

- Inner VIF Values

	Attitude	Intention to Adopt	Perceived Compatibility	Perceived Ease of Use	Perceived Enjoyment	Perceived Usefulness	Perceived controllability	Sacrifices
Attitude		1.100						
Intention to Adopt								
Perceived Compatibility				1.015		1.001		
Perceived Ease of Use	1.000					1.001		
Perceived Enjoyment				1.060				
Perceived Usefulness		1.103						
Perceived controllability				1.053				
Sacrifices		1.025						

- F Squared

	Attitude	Intention to Adopt	Perceived Compatibility	Perceived Ease of Use	Perceived Enjoyment	Perceived Usefulness	Perceived controllability	Sacrifices
Attitude		0.227						

Intention to Adopt								
Perceived Compatibility				0.005		0.000		
Perceived Ease of Use	0.304					0.322		
Perceived Enjoyment				0.154				
Perceived Usefulness		0.101						
Perceived controllability				0.007				
Sacrifices		0.102						

APPENDIX 6 - SUMMARY OF THE TRANSCRIPTS OF THE VARIOUS INTERVIEWS CONDUCTED.

The interviews were conducted in French and have therefore been translated into English for the sake of this work. Some passages, less critical, were not transcribed/translated and the transcription of the interviewees was proposed to revision to the interviewees.

Interview 1 - Smart Home Owner (Online video interview on Saturday, June 13, 2020 at 2pm)

- Greetings of use

- Explanation of the study conducted and definition of important terms

Can you introduce yourself and explain your relationship with new technologies?

Of course, my name is Michel, I am 56 years old and I am a fervent lover of new technologies. I live with my wife in a house on the outskirts of Brussels. I connected my house a few years ago. I have always been passionate about new technologies and I try again and again to stay up to date and adopt the technologies that I find useful and that could simplify my life. That's why connected objects quickly attracted me.

How did your interest in IoT and the connected home appeared?

I forgot to mention in my presentation that I have my own business. I had been interested in some time in buying connected cameras (CCTV) to keep my business safe. I then tried to make objects interact with them using multiple tools such as Raspeberries Pi and Arduinos if you know what they are in order to build myself what I needed. At home, I quickly adopted a Google Home and therefore I quickly wanted to automate my daily activities. I started by acquiring a "Tahoma" box from Somfy so that I could create scenarios for closing my shutters. To give you an example, when I go to sleep, all I have to do is ask Google to close all the shutters and I can go to sleep peacefully. Moreover, when I go on a trip, I can simulate my presence remotely because I also have connected light bulbs which I admit I don't know the brand (I bought them at Kruitvat if I recall correctly).

How does your entourage react to your interest in new technologies and in particular to your home?

I only live at home with my wife since my son left the house few years ago. She is very happy to be able to automate some of her tasks even if she was skeptical at first, now she has adopted her Google assistant as she calls it. As for my friends, they are often impressed by the installation and ask me a lot of advice on this level. There's a certain curiosity that often emanates even if some people find it a bit gadget-like and not very useful. I think it really lacks a flagship product that would show everyone how much time is saved everyday thanks to connected objects. When talking about connected objects, people don’t often know all the spectrum of products available and what can be done. I fact I don’t know it myself.

What activities would you like to automate in your home?

I have to say that I think I've already automated most of the things I was thinking about when I started connecting my house. The only thing I can think of right now would be automating my garage door so that it opens when I drive home with my car. I will certainly look for a solution once this virus has finally left us.

From your view what might these smart devices bring to you and your home? What makes people adopt them?

Personally, I am convinced that these objects help me feel better in my home and increase my comfort, a perfect example is the connected thermostat I have which allows me to heat my home the way I want and even allows me to make small savings which is always nice. What I love about these things too is that I can manage them from anywhere as soon as I have 4G. When I am at work I can check if I have forgotten to turn off the lights in a room or if someone rings the doorbell, I can immediately communicate with them via the door phone connected to my local internet network.

What do you see as a challenge in the connected object sector and more specifically in the connected home sector?

The first thing that comes to mind is the incompatibility between many objects on the market. For a person who knows nothing about it, it's difficult to know if the objects he wants to buy are compatible and even if they are in theory, it's sometimes difficult to do it in practice and these objects are often expensive though. Then I think that the security of the data we transmit to companies is a real challenge but this one is not specific to IoT as we often see

with social networks and everything related to the internet in general. I think that's about it, yes, lack of standardization and privacy I would say.

- End of the interview and proposal for transcription.

Interview 2 - Potential Future Smart Home Owner (Online video interview on Friday, July 10, 2020 at 6pm)

- Greetings of use

- Explanation of the study conducted and definitions of important terms

Could you introduce yourself and explain your relationship with new technologies?

As you already know, my name is Jonathan, I'm 30 years old and I work for the STIB. Otherwise I live in an apartment in the center of Brussels. Concerning new technologies I think I am like every young person of my age, I am very interested but I rarely have the budget to test new products such as virtual reality helmets, AR etc... but I feel a particular attraction to this type of products...

Do you have a special attraction to connected objects? And if so, do you already own them, or do you plan to acquire them in the future?

According to your definitions yes, I am attracted by this technology but no I don't own it at the moment as I rent my apartment, I don't want to invest in it. I'm currently looking for land to build my house and I think it's the perfect opportunity to design it to be connected but I'm still hesitating.

Why are you hesitating?

I don't really know of any companies that offer to intervene during the construction of a house so that it can be connected immediately once it is built. Perhaps you have some advice on this?

(...)

Another thing that also worries me is the price it would cost me, I would already have to borrow a large amount of money from my bank and I would hardly be able to pay more for my house to be connected.

Do you already have ideas about what you would like to automate in your future home?

I have a friend who has Philips Hue lights and it gives a very nice atmosphere, I think. Otherwise anything that allows me not to do chores would certainly please me a lot. I've seen

that there are vacuums that detect when you're not at home and that go off to clean rooms in the house, it's great this thing! (...) All in all I would say anything that can save me time in boring and repetitive tasks.

When you think about connected objects and the connected home, what do you think could be a brake on adoption?

First of all, the price, I think it's new and it must still be relatively expensive. I think that data security must be a brake even if I must admit that personally I don't fear it too much. Another thing that comes to mind is that I find that for the moment it is often up to humans to adapt their habits to the machine when it should be the opposite. Then I have to say that I don't see what connected object I couldn't do without, except the vacuum cleaner because I'm lazy (laughs) there isn't really a flagship product except maybe Google Home, but I don't really know what you can do with that. There really should be a product that greatly enhances comfort and that people see as a must-have or "in fashion" so that they buy other connected objects and connect their home little by little.

- End of the interview and suggested transcription

Interview 3 - Smart Home Refractory (Online video interview on Tuesday, June 23, 2020 at 4:30 p.m.)

- Greetings of use

- Explanation of the study conducted and definitions of important terms

Could you introduce yourself and explain your relationship with new technologies?

Of course, so I'm Monica, I'm 42 years old and I live in a house in a small village near Grez-Doiceau in which I moved recently with my companion. I have two daughters, one is working and the other is still at university, so they don't live at home anymore. I work as a sales representative in a company in Brussels. My relationship with technology is very limited, I would say. At home we don't have a television, apart from our smartphones and the computer in front of which I'm talking, we don't have a lot of technology at home.

What is your overall opinion on connected objects and the smart home?

I don't know a lot about it as I'm not very interested in this technology. I think we are far too connected throughout our working day and it's good to disconnect a bit when we get home. It's stressful to always have information about everything and anything. I think it's a phenomenon that's growing quite a bit by the way. People who work in the city like I do and come home at night have a real desire to think about something else. I'm also a fan of "digital detox", do you know what it is? (Explanation of the phenomenon)

So why do you think people are adopting this technology and why do you think some people want to automate certain activities within their homes?

I don't know, I would certainly say for the aesthetic side but for me it's all gadgetry and it's not useful for much but then, I certainly don't know enough about it. If people buy it, it must be useful for them but not for me.

Would there be a connected object that could make you change your mind and that you think you would want to integrate into your home?

No, I don't see any sorry. Again, I'm not an expert, but I think that these connected objects are not very healthy either because of the waves they constantly produce, so it's difficult for me to want to adopt them and even more so if it's for inside my home. I have already had health issues and one reason for I moved recently is the construction of a phone antenna near my old house. So, I am absolutely not the target of this kind of product, I think.

What do you think are the biggest barriers to the adoption of technology?

As I said, I think health concerns can be a challenge for connected objects. Then the digital detox trend could also impact the success of the connected home and its objects. (...) Finally, I also suppose that these objects have a certain price and it is certainly dangerous to use them. We hear a lot about data scandals I guess there must have been a lot of data scandals on such objects.

I hope that despite my low interest for connected objects I could have brought you some interesting elements for your work good luck.

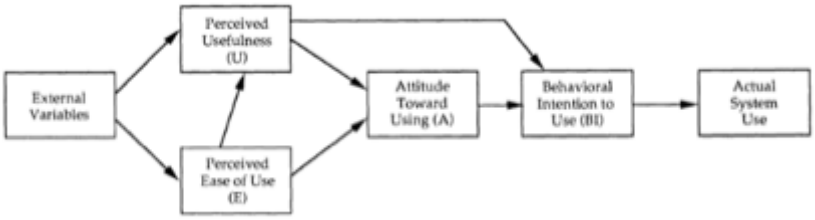
- End of the interview and proposal for a transcript

APPENDIX 7 - TECHNOLOGY ACCEPTANCE MODEL (TAM)

In this Appendix we provide a more elaborate review of the TAM.

An often-mentioned model to study user adoption of a technology is the Technology Acceptance Model (TAM). First developed in (Davis, 1989), the TAM was adapted from the initial Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1975; Ajzen & Fishbein, 1980) in order to specifically explain Information Technology (IT) systems usage. The TAM is based on the TRA for specifying causal linkages between two key beliefs: perceived usefulness and perceived ease of use, and users' attitudes, intentions and actual computer adoption behavior (Davis, Bagozzi & Warshaw, 1989). Perceived ease of use corresponds to "the degree to which a person believes that using a particular system would be free of effort" and perceived usefulness to "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989). In addition, Davis (1989) states that the perceived usefulness of a system is influenced by its ease of use because the easier it is to use a system, the less effort it requires, and the more useful it becomes. Also, Davis (1989) highlighted that perceived usefulness and perceived ease of use were significantly correlated

with, not only current usage (in a first study), but also with future usage (in a second study). Davis, Bagozzi and Warshaw (1989) state that "all else being equal, people form intentions to perform behaviors toward which they have positive affect", which highlights the link between attitudes (the general impression of the technology) and behavioral intentions.



First version of the TAM as presented in Davis, Bagozzi & Warshaw (1989).

The TAM is commonly used to explain an individual's acceptance of a technology because: it was empirically validated by Davis (1989), it has been backed by a wide amount of reviews and empirical research (e.g. Hu et al., 1999; Moon & Kim, 2001), it is simple (small amount of factors), it is applicable to a wide variety of contexts, and the factors used are simple, specific, easy to use and easy to understand.

Nevertheless, the TAM has been studied a lot and improved models have emerged. The most notable improvements are: the TAM 2 (Venkatesh & Davis, 2000; Venkatesh, 2000), the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003), and the TAM 3 (Venkatesh & Bala, 2008).

TAM 2:

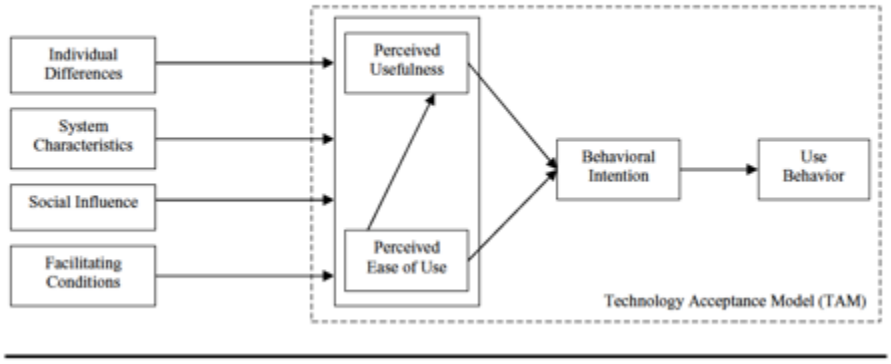
Venkatesh and Davis (2000) developed the TAM 2 by identifying and defining the main determinants of perceived usefulness. Subjective norm, image, job relevance, output quality, result demonstrability, and perceived ease of use, as well as two moderating variables (i.e. voluntariness and experience) were identified and empirically validated as determinants of perceived usefulness. In parallel, research was done concerning perceived ease of use. Venkatesh (2000) states that system users will form early perceptions of perceived ease of use based on several anchors related to their own general beliefs regarding computers and computer use. The anchors identified by Venkatesh (2000) of perceived ease of use are: computer self-efficacy, perception of external control, computer anxiety, computer playfulness, perceived enjoyment, and objective usability. Venkatesh (2000) also notes that the effects of these anchors are not frozen in time. Indeed, while these anchors drive initial judgments of perceived ease of use, adjustments are made by individuals as they gain hands-on experience with the new system. In that sense, with increasing experience, computer playfulness and computer anxiety are expected to decrease whereas perceived enjoyment and objective usability are expected to increase. Computer self-efficacy and perceptions of external control are predicted by Venkatesh (2000) to remain strong over time. Respective definitions of perceived usefulness and perceived ease of use determinants can be found in the next table.

Perceived usefulness determinants, as identified in (Venkatesh & Davis, 2000)	Perceived ease of use	The degree to which a person believes that using an IT will be free of effort (Davis et al., 1989).
	Subjective norm	The degree to which an individual perceives that most people who are important to him think he should or should not use the system (Fishbein & Ajzen, 1975; Venkatesh & Davis, 2000).
	Image	The degree to which an individual perceives that use of an innovation will enhance his or her status in his or her social system (Moore & Benbasat, 1991).
	Job relevance	The degree to which an individual believes that the target system is applicable to his or her job (Venkatesh & Davis, 2000).
	Output quality	The degree to which an individual believes that the system performs his or her job tasks well (Venkatesh & Davis, 2000).
	Result demonstrability	The degree to which an individual believes that the results of using a system are tangible, observable, and communicable (Moore & Benbasat, 1991).
Perceived ease of use determinants, as identified in (Venkatesh, 2000)	Computer Self-Efficacy	The degree to which an individual believes that he or she has the ability to perform a specific task/job using the computer (Compeau & Higgins, 1995a, 1995b).
	Perception of External Control	The degree to which an individual believes that organizational and technical resources exist to support the use of the system (Venkatesh et al., 2003).
	Computer Anxiety	The degree of "an individual's apprehension, or even fear, when she/he is faced with the possibility of using computers" (Venkatesh, 2000, p. 349).
	Computer Playfulness	". . .the degree of cognitive spontaneity in microcomputer interactions" (Webster & Martocchio, 1992, p. 204).
	Perceived Enjoyment	The extent to which "the activity of using a specific system is perceived to be enjoyable in its own right, aside from any performance consequences resulting from system use" (Venkatesh, 2000, p. 351).
	Objective Usability	A "comparison of systems based on the actual level (rather than perceptions) of effort required to completing specific tasks" (Venkatesh, 2000, pp. 350–351).

Determinants of perceived usefulness and perceived ease of use.

The determinants of perceived usefulness and perceived ease of use can also be categorized in four different types of determinants: individual differences, system characteristics, social influence, and facilitating conditions (see Figure below). Please refer to the table below for their definition.

Figure 1: Theoretical framework.



Types of determinants that influence perceived usefulness and perceived ease of use, as theorized in Venkatesh & Davis (2000).

Further, the TAM 2 presents social influence and cognitive instrumental processes as the theoretical processes that explain the influence of the various determinants on perceived usefulness and behavioral intention. Three social influence mechanisms that help understand social influence processes are identified: compliance, internalization, and identification. Compliance refers to when an individual adapts his behavior in order to avoid punishment or to get a reward (Miniard & Cohen, 1979). Identification refers to an individual's belief that performing a behavior will elevate his own social status to the social status of a referent group because important referents believe that behavior should be performed (Venkatesh & Davis, 2000). Internalization refers to the incorporation of a referent's belief into one's own belief structure (Warshaw, 1980). Subjective norm and image are the social influence processes linked to perceived usefulness. TAM 2 expects that subjective norm positively influences perceived usefulness through internalization whereas image is stated to positively influence perceived usefulness through identification processes. With increasing experience, the effect of subjective norm on perceived usefulness and behavioral intention is supposed to decrease. Concerning cognitive instrumental processes, they are based on the idea that individuals "form perceived usefulness judgment in part by cognitively comparing what a system is capable of doing with what they need to get done in their job" (Venkatesh & Davis, 2000, p. 190). From there, the TAM 2 identifies perceived ease of use and result demonstrability as direct positive influencers of perceived usefulness. In addition, it states that the higher the output quality, the higher the effect of job relevance on perceived usefulness will be.

Determinant Type	**Definition**
Individual differences	Personality and/or demographics (e.g., traits or states of individuals, gender, and age) that can influence individuals' perceptions of perceived usefulness and perceived ease of use (Venkatesh & Bala, 2008).
System characteristics	Salient features of a system that can help individuals develop favorable (or unfavorable) perceptions regarding the usefulness or ease of use of a system (Venkatesh & Bala, 2008). Perceived usefulness determinants falling into this category: job relevance, output quality, result demonstrability, perceived ease of use.
Social influence	Various social processes and mechanisms that guide individuals to formulate perceptions of various aspects of an IT (Venkatesh & Bala, 2008). Perceived usefulness determinants falling into this category: subjective norm and image determinants
Facilitating conditions	Organizational support that facilitates the use of an IT (Venkatesh & Bala, 2008).

Definitions of the different types of determinants.

TAM 3 :

The TAM 2 provided a strong theoretical base to explain user adoption of new IT systems. However, a lack of practical guidance for practitioners was one of the most common criticisms (Lee, Kozar, & Larsen, 2003). Hence, the TAM 3 (Venkatesh & Bala, 2008) was aimed at identifying the potential interventions that could be done pre- and post-implementation of new systems, in order to influence the determinants of perceived usefulness and perceived ease of use. By doing so, the TAM 3 could be used as guiding tool for managers to make effective decisions regarding interventions. Additionally, the TAM 3 provides further research points that can be addressed to enhance managerial interventions.

Moreover, Venkatesh and Davis (2000) had identified and presented the general determinants of perceived usefulness in the TAM 2, Venkatesh (2000) had identified the determinants of perceived ease of use. These two works had been done separately and therefore the link between both had not been set yet. Venkatesh and Bala (2008), in the TAM 3, therefore presented an integrated model encompassing determinants of both perceived ease of use and perceived usefulness, as well as studied possible crossover effects between both.

Hence, the TAM 3 is an integrated model of technology acceptance that: groups the determinants of perceived ease of use and perceived usefulness (nomological network), empirically tests the proposed model, and suggests potential pre-and post-implementation interventions that can be broadly applied to foster employee adoption of new IT systems.

Concerning the integration of perceived ease of use and perceived usefulness in the model, Venkatesh and Bala (2008) posit that no cross-over effects exist between the determinants of those two factors. In other words, in the TAM 3 the determinants of perceived usefulness will not influence perceived ease of use and reciprocally. As stated earlier, two theoretical processes affect the determinants of perceived usefulness: social influence (i.e. compliance, identification, and internalization) and cognitive instrumental processes (Venkatesh & Davis, 2000). Venkatesh and Bala (2008) suggest that even if an individual gets information from important referents about how easy a system is to use, it is unlikely that the individual will form stable perceptions of ease of use based on the beliefs of referent others over and above his or her own general computer beliefs and hands-on experience with the system. (Venkatesh & Bala, 2008, p.8)

Hence, the social influence process (characterizing the determinants of perceived usefulness) is not strong enough to outweigh the personal anchors that influence the perception of ease of use. Therefore, the determinants of perceived usefulness are believed to not significantly influence the perceived ease of use (Venkatesh & Bala, 2008).
In the other way, the influence of the determinants of perceived ease have been shown to not significantly influence perceived usefulness (Venkatesh & Bala, 2008). Determinants of perceived ease of use are primarily individual differences variables and general beliefs about

the system and system use (i.e. control beliefs, intrinsic motivation, and emotion) (Venkatesh, 2000). Perceived usefulness, on the contrary, is "an instrumental belief that is conceptually similar to extrinsic motivation and is a cognition (as opposed to emotion) regarding the benefits of using a system" (Venkatesh & Bala, 2008). Hence, the determinants of perceived ease of use (i.e. perceptions of control, enjoyment, playfulness, and computer anxiety) do not provide a basis to form perceptions of instrumental benefits of using a system (Venkatesh & Bala, 2008).

Another theoretical contribution of the TAM 3 is the use of experience as moderating effect of some of the relationships.
Venkatesh & Bala (2008) find that perceived ease of use and usefulness are moderated by experience. First, they suggest that more hands-on experience with a system should give the user more information on how easy or difficult the system is to use, hence experience should increase the perceived ease of use of a system. Then, it is assumed that perceived ease of use will be valued by users when forming perceptions about usefulness (Venkatesh et al., 2003), hence experience with the system would (indirectly) influence perceived usefulness. Their argument is based on the action identification theory (Vallacher and Kaufman, 1996), where high-level identities are distinguished from low-level identities. High-level identities are related to individuals' goals and plans whereas low-level identities are linked to the means to achieve these goals and plans. Perceived ease of use is considered as a low-level identity whereas perceived usefulness is considered as a high-level identity (Davis & Venkatesh, 2004; Venkatesh & Davis, 2000). Venkatesh and Bala (2008) suggest that users will use their experience gained from low-level actions (i.e. perceived ease of use) to better assess their likelihood of attaining high-level goals (i.e. perceived usefulness). Hence, the influence of perceived ease of use on perceived usefulness increases with experience. This was empirically tested and validated by Venkatesh and Bala (2008).

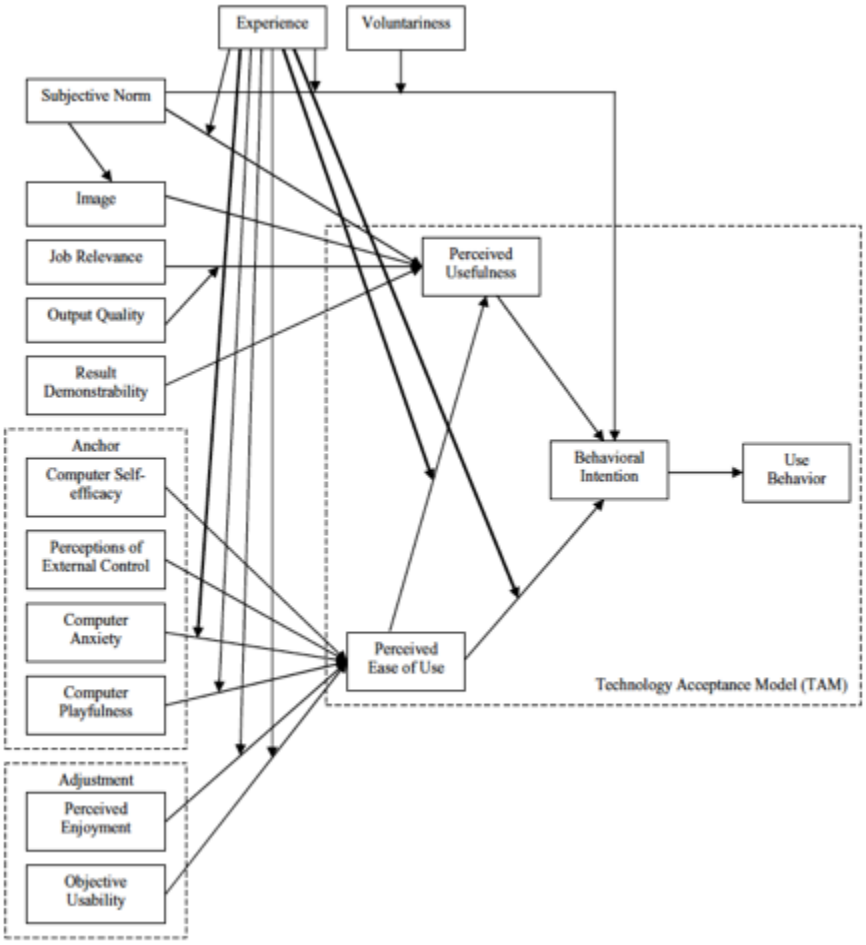
Venkatesh and Bala (2008) also posit that the influence of **computer anxiety on perceived ease of use is moderated by experience**. Computer anxiety is an anchoring belief that negatively affects the perception of ease of use (Venkatesh, 2000). The role of anchors is believed to diminish over time as adjustment information (i.e. experience) becomes available (Yadav, 1994; Wasnik, Kent, & Hoch, 1998; Mussweiler & Strack, 2001). Therefore, the effect of computer anxiety on perceived ease of use is expected to decline with increasing experience as users will have more accurate perceptions of how difficult it is to use the system (Venkatesh & Bala, 2008). It is also expected that with increasing experience, general computer beliefs vanish and become less important than system-specific beliefs and perceived enjoyment, as users become more aware of the effort required by the system and discover system features that lead to enjoyment (Venkatesh, 2000).

Another contribution of Venkatesh and Bala (2008) is to highlight that the relationship from perceived ease of use to behavioral intention is moderated by experience. Venkatesh (2000) states that while perceived ease of use can be a hurdle for system users at the beginning, it decreases over time as they become accustomed to the system. The effect of perceived ease of use on behavioral intention to use the system will therefore become less important (i.e. decrease) to users, as they get increasing hands-on experience (Venkatesh and Bala, 2008).

Moreover, Venkatesh and Bala (2008) confirmed some of the findings made by Venkatesh and Davis (2000) concerning perceived usefulness. They found: perceived ease of use, subjective norm, image, and result demonstrability to be significant predictors of perceived usefulness at all time periods, the effect of job relevance on perceived usefulness became stronger when output quality increased, the effect of subjective norm on perceived usefulness decreased when experience increased, and the effect of image on subjective norm remained significant at all time periods.

Concerning the determinants of perceived ease of use, Venkatesh and Bala (2008) found that anchors (i.e. computer self-efficacy, perceptions of external control, computer anxiety, and computer playfulness) were significant determinants of perceived ease of use, at all times. The adjustments (i.e. perceived enjoyment and objective usability) became significant over time. Also, it was found that none of the determinants of perceived usefulness had significant influence on perceived ease of use and that the effect of computer anxiety on perceived ease of use became weaker with increasing experience.

In relation with behavioral intention, Venkatesh and Bala (2008) found that: perceived usefulness had the most influence on behavioral intention, the effect of perceived ease of use on behavioral intention became weaker when experience increased, and the effect of subjective norm on behavioral intention also became weaker with increasing experience, especially in the voluntary context.



TAM 3 as presented in Venkatesh & Bala (2008).

Since one of the goals of the TAM 3 is to provide guidance for practitioners, Venkatesh and Bala (2008) suggest possible interventions, based on the rich theoretical understanding of the determinants of IT adoption and use. Those interventions are divided into two groups: pre-implementation interventions corresponding to the different stages leading to the roll-out of the new system, and post-implementation interventions that relate to the actual deployment of the system. The stages and substages, inspired from Cooper and Zmud (1990) and Saga and Zmud (1994), can be found in the following table.

Phase	**Subphase**	**Definition**
Preimplementation	Initiation	Identification of organizational problems/opportunities that warrant a technology solution
Preimplementation	Organizational adoption	Organizational decision to adopt and install a technology
Preimplementation	Adaptation	Modification processes directed toward individual/organizational needs to better fit the technology with the work setting
Post implementation	User acceptance	Efforts undertaken to induce organizational members to commit to the use of technology
Post implementation	Routinization	Alterations that occur within work systems to account for technology such that these systems are no longer perceived as new or out-of-the ordinary
Post implementation	Infusion	Technology becomes more deeply embedded within the organization's work system

Definitions of the different subphases of implementation, as theorized in Venkatesh & Bala (2008).

As the goal of these interventions are to influence the determinants of perceived ease of use and perceived usefulness, each intervention has a specific influence on each determinant and therefore some interventions are more suited for influencing particular determinants. Venkatesh and Bala (2008) therefore provide a framework that can be used as overview of the different interventions and their respective purposes.

Table 9: Summary of interventions[a].

	Preimplementation Interventions				Postimplementation Interventions		
	Design Characteristics	User Participation	Management Support	Incentive Alignment	Training	Organizational Support	Peer Support
Determinants of Perceived Usefulness							
Subjective Norm		X	X	X			X
Image			X	X			X
Job Relevance	X	X	X	X	X	X	X
Output Quality	X	X	X	X	X	X	X
Result Demonstrability	X	X	X	X	X	X	X
Determinants of Perceived Ease of Use							
Computer Self-Efficacy					X		
Perceptions of Ext. Control		X	X			X	X
Computer Anxiety		X			X	X	
Computer Playfulness		X			X		
Perceived Enjoyment	X	X		X	X		
Objective Usability	X	X			X		

[a]X indicates a particular intervention can potentially influence a particular determinant of perceived usefulness or perceived ease of use.

Potential interventions depending on implementation stage and determinant to influence as presented in Venkatesh and Bala (2008).

The suggested pre-implementation interventions pursue two goals: minimization of initial resistance and providing a realistic preview of the system. Venkatesh and Bala (2008) propose pre-implementation interventions related to design characteristics, user participation, management support, and incentive alignment.
Design characteristics are divided into two groups: information-related characteristics, and system-related characteristics. The information-related characteristics should be designed in order to help system users take better decisions (by providing timely, accurate and understandable information) so that important determinants of perceived usefulness (i.e. greater job relevance of the system, high output quality, and greater result demonstrability) are positively influenced. On the other side, system-related characteristics such as a reliable, flexible, and user-friendly system should be designed to positively influence important determinants of perceived ease of use (i.e. increase enjoyment and reduce computer anxiety).

Besides design characteristics, user participation in the system development and implementation activities (e.g. system evaluation and customization, prototype testing) should also be encouraged as it can favorably influence the users' judgments about job relevance, output quality, and result demonstrability (Venkatesh & Bala, 2008). Venkatesh and Bala (2008) also suggest that participation through hands-on activity may reduce anxiety and favorably influence perceptions of external control, perceived enjoyment, and objective usability.

Further, Venkatesh and Bala (2008) note that effective management support, in the form of communication, involvement and commitment to system implementation, can have an impact on the users' perceptions of subjective norm and image as well as on users' perceptions of job relevance, output quality, and result demonstrability.
In addition, a key factor in successful implementation of new systems is incentive alignment. Ba et al. (2001) argue that proper software engineering and technology acceptance might not

be sufficient to reap the benefits of a new system, as system features and capabilities should also be perceived by their users as aligned with their own interests and incentives.

Venkatesh and Bala (2008) also identify the following post-implementation interventions as crucial for influencing the determinants of technology acceptance: training, organizational support, and peer support.

Managers need to apply the aforementioned interventions depending on the context (e.g. implementation stage, type of system). Interventions that will influence the determinants of perceived usefulness (e.g. design characteristics, user participation, incentive alignment, training, organizational and peer support) seem to be the most relevant in a voluntary context whereas interventions aimed at influencing determinants of perceived ease of use (e.g. design characteristics, user participation, training, and peer support) will be of more importance for complex systems (Venkatesh & Bala, 2008).
Managers can also allocate resources and prioritize interventions based on the impact of these interventions on different determinants of technology adoption (Venkatesh & Bala, 2008).

APPENDIX 8 - VALUE-BASED ADOPTION MODEL (VAM)

The VAM was proposed in (Kim et al., 2007) and argued that the TAM was limited in explaining acceptance of new ICT. More specifically, Kim et al. (2007) pointed out that individuals studied in the TAM were employees in an organizational setting and therefore considered as technology users, whereas in the VAM individuals are not only users but also consumers. The importance to take into consideration such social aspects (e.g. user characteristics and environment) in order to better understand smart home adoption was also expressed in (Ginter, 2001) and (Yang, Lee & Lee, 2018).

The technologies studied with TAM can be considered traditional technologies whereas the VAM is more adapted to new ICT. The use of technology in the TAM is done for work purposes and its usage is borne by the company, whereas the VAM allows to study new technology adoption and usage for personal purposes and usage is therefore borne by the individuals (Kim, Park & Choi, 2017).
TAM uses perceived usefulness and perceived ease of use to explain intention to use whereas VAM uses perceived value – influenced by perceived sacrifices and perceived benefits – to explain intention to use (see Figure). The perceived benefits in the general VAM are themselves mainly influenced by perceived usefulness and perceived enjoyment while the sacrifices are mainly influenced by perceived technicality and perceived fee.
Moreover, the VAM adopts a cost-benefit paradigm, where comparing the cost of uncertainty is used for deciding whether to use a new technology (Lin et al., 2012). In other words, the VAM aims to explain adoption of new technologies by combining the original TAM (Davis et al., 1989) with the theory of perceived value of Zeithaml (1988).

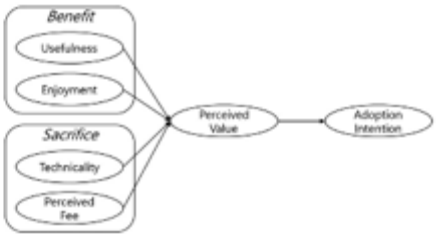


Figure 1. Value-based Adoption Model (Kim et al., 2007).

Value-Based Adoption Model from Kim et al. (2007).

The Elaboration Likelihood Model (ELM) serves as inspiration for constituting the factors contained in the VAM. It therefore seems relevant to briefly explain the ELM.

The ELM was first developed in (Petty & Cacioppo, 1986) and relies on a dual process theory (see figure below). The dual process theory describes how people accept and process information. Two different routes exist – central route and peripheral route – and people's attitude will decide which path will be chosen, for each specific situation. When using the central route, individuals will carefully review new information and balance its merits and weaknesses, as well as its significance (Petty & Cacioppo, 1986). On the other side, the peripheral route offers a fast way to process information by accepting or refusing information without active thinking. Those swift decisions are influenced by the peripheral cues (Petty & Cacioppo, 1986). The elaboration likelihood will decide on which route to take, depending on the individual's amount of motivation and ability to process the new information. If the individual is able to actively think and spend some cognitive effort, the central route will be taken. If not, the peripheral route will be taken as it requires less cognitive effort (Petty & Cacioppo, 1986). When using the ELM to identify potential determinants of perceived benefits and perceived sacrifices, it must be taken into consideration that in general individuals do not think in a single process – take only either the central route or peripheral route -- but rather in dual processes, where the central and peripheral routes are alternated (Petty & Cacioppo, 1986).

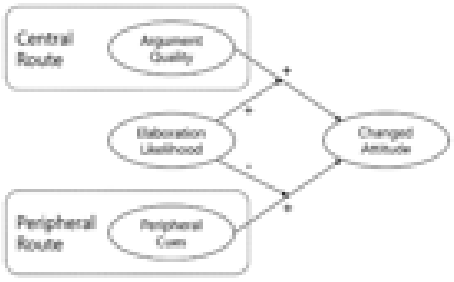


Figure 2. Elaboration Likelihood Model (Petty & Cacioppo, 1986).

Elaboration Likelihood Model (ELM) elaborated by Petty & Cacioppo (1986).

Other dual process models have been developed in the literature, amongst which System 1 and System 2 of Kahneman (2011) and the reflective and impulsive determinants of social behavior of Hofmann, Strack and Deutsch (2004).

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/lsm**