AN INVESTIGATION INTO THE SECURITY CHALLENGES AND IMPLICATIONS SURROUNDING SMART HOME TECHNOLOGIES

A dissertation submitted in partial fulfilment of the requirements for the - degree of Bachelor of Science (Honours) in Computing

By

Student Name: Tajred Alean M Alaswad
Student ID: ST20092614
Supervisor: Dr. Taslima Begum
Department of Computing & Information Systems
Cardiff School of Management
Cardiff Metropolitan University

April 2017
Acknowledgement

Primarily, I am thankful to my supervisor Dr. Taslima Begum for the continuous support, encouragement, motivation, patience, and guidance. This project is not possible without my supervisor.

I would never have been able to complete my project without the assistance of my family. I thank my friends for their encouragement with their best wishes. Finally, I would like to thank Allah for his mercy and grace during my project.

My thankfulness extends especially to my batch mates their co-operation, which they offered me in making this, report a success. I would also like to convey my sincere gratitude to the library and laboratory staff, for providing me the relevant reading materials and other resources which indeed helped to a great extent to accomplish my goal of creating an accurate, relevant and an affluent report successfully.
Abstract

A smart home is typically a new home that has uniquely structured wiring or wireless that allows residents to remotely control or program a variety of mechanised home electronic gadgets by inputting a single command (Jiang 2004). For instance, a property owner out of town can make use of a Touchtone phone to set up a home security system, switch gadgets on or off, control temperature gauges, program an entertainment system or home theatre, control lighting and carry out many other tasks. The field of home computerisation is growing quickly as electronic advances unite, however, the increased use of Smart Home technologies has raised many new security concerns for users.

This dissertation uses both qualitative and quantitative data to better understand the security issues around smart home technologies. An interpretative research philosophy is adopted involving an inductive research strategy for gathering qualitative data. Questionnaires (survey) and interviews are used to collect primary data and were developed from the analysis of current literature within this domain.

From the quantitative and qualitative analysis conducted it is identified that there are security concerns and threats available for the end users of the smart home technologies. Also, this report provides some valuable recommendations not just for the end users but also for the manufacturers of the technology to reduce the security concerns.
# Table of Contents

Acknowledgement ........................................................................................................... 1

Abstract ............................................................................................................................... 2

1.0. Introduction ..................................................................................................................... 6

1.1. Aim and Objectives ......................................................................................................... 6

1.1.1. Aim .......................................................................................................................... 6

1.1.2. Objectives ............................................................................................................... 6

1.2. Scope ............................................................................................................................... 7

1.3. Research question .......................................................................................................... 7

1.4. Report Structure ............................................................................................................ 7

2.0. Literature Review .......................................................................................................... 8

2.1. Introduction .................................................................................................................... 8

2.2. Smart Home Systems ..................................................................................................... 9

2.3. Smart Home Software and Technology ......................................................................... 9

2.4. Setting Up a Smart Home .............................................................................................. 11

2.5. Advantages of Smart Home ......................................................................................... 11

2.6. Smart Home Security .................................................................................................... 12

2.6.1. Smart Home Fire Protection ................................................................................... 12

2.6.2. Access Control ........................................................................................................ 12

2.6.3. Artificial Intelligence Programs Protect the Home owner ...................................... 13

2.7. Technology and Research in Smart Home Security ..................................................... 13

2.7.1. Smart Home Networks User Verification Using Neural Network ......................... 13

2.7.2. Sentry@Home ........................................................................................................ 13

2.7.3. Defending DDoS Attacks Caused by Spam ............................................................ 14

2.8. Conclusion .................................................................................................................... 14

3.0. Methodology ................................................................................................................. 16

3.1. Secondary Research ..................................................................................................... 16

3.2. Primary research .......................................................................................................... 16

3.2.1. Selection of participants in the survey .................................................................... 17

3.2.1. Approaches used for the research ......................................................................... 18

3.2.3. Method Used in Collecting Information ................................................................ 19

3.2.4. Survey Questions types ......................................................................................... 20

3.3. Survey and Interview Analysis ..................................................................................... 20
3.4. Questions used for Interview and survey .......................................................... 21

The purpose for selecting the questions for interview and survey is shown in table XX ........ 21
3.5. Steps taken to arrive at the recommendation ................................................... 22
4.0. Findings and Analysis ......................................................................................... 23
4.1. Introduction ........................................................................................................ 23
4.2. Interview Analysis ............................................................................................ 23
4.3. Survey Analysis ................................................................................................. 24

4.3.1. Personal Information .................................................................................. 24
4.3.2. Smart Home Experience ............................................................................ 26
4.3.3. Priorities with respect to Smart Home Technologies ................................. 27
4.3.4. Security issues faced from Smart Home technologies .............................. 28
4.3.5. Recommendations to reduce the security issues ........................................... 29
5.0. Recommendation ............................................................................................... 31
5.1. Introduction ...................................................................................................... 31
5.2. Recommendation for Manufacturers ............................................................... 31
5.3. Recommendation for end users ....................................................................... 33
6.0. Conclusion and Future works ........................................................................... 34

6.1. Objective analysis ............................................................................................ 34
6.2. Future work ...................................................................................................... 34
6.3. Limitations ........................................................................................................ 35
7.0. References ......................................................................................................... 36

APPENDIX: Ethics Approval Email ............................................................................ 38

List of Tables
Table 1: Advantages and disadvantages of mixed methodology (Tashakkori and Teddlie, 1998) ................ 16
Table 2: The critical assessment of qualitative and quantitative research methods ................... 17
Table 4: Critical assessment of each method used .................................................................. 18
Table 5: Reasons for selecting these mediums for the interview ........................................ 19
Table 6: The reason for selecting these methods to gather responses for the survey ........................ 19
Table 7: Critical Analysis on open-ended and Closed-ended questions (Lavarakas, 2008) .............. 20
Table 8: Questions and reasons .................................................................................... 21
Table 11: Recommendation list for Smart Home technology manufacturers .......................... 31
Table 12: Recommendation for Smart home technology end users ................................... 33

List of Figures
Figure 1: Survey question1 Analysis ........................................................................... 24
Figure 2: Survey question2 Analysis ........................................................................... 25
Figure 3: Survey question3 Analysis ........................................................................... 25
1.0. Introduction
The Internet of Things (IoT) is the network or connection of physical components or things or devices. There are several real-world applications of IoT currently available, namely smart parking, noise urban charts, waste management, smart lighting, quality of water, leakages of water, detection of forest fire, smart grid, water flow, level of tank, supply chain control, NFC payment mode, M2M applications, ozone presence, infant care, smart village, and smart health management. The technologies used for IoT are Radio Frequency Identification Device (RFID), EnOcean, NFC, Bluetooth, Wi-Fi, Weightless (SIG), Global System for Mobile communications (GSM), IPV4/IPV6 IPV- Internet Protocol Version), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), 6LoWPAN, and so on.

Currently, there is an increase in the use of IoT applications and connecting the components online. As more devices become accessible from the internet, the security implications of these devices become more critical, as the number of possible attack vectors increases. A Smart home is one of the major applications of the Internet of Things. Smart Home plainly emerges, positioning as most noteworthy Internet of Things application on every single measured channel. More than 60,000 individuals right now hunt down the expression "Smart Home" monthly. This is not surprising (Chan, 2009). The IoT Analytics organization database for Smart Home incorporates 256 organizations and new companies. A bigger number of organizations are dynamic in keen home than some other application in the field of IoT. The aggregate sum of financing for Smart Home new businesses right now surpasses $2.5bn. This rundown incorporates conspicuous start-up names, for example, Nest or Alert-Me and also various multinational enterprises like Philips, Haier, or Belkin (Aldrich, 2003).

This project mainly focusing on the security issues that can be faced by the end user when they use the smart home technologis and the methods in which the provider and the end user can minimise or reduce the security issues. This is achieved conducting secondary and primary research in this project. The recommendations how to keep the Smart home is derived from the research.

1.1. Aim and Objectives
1.1.1. Aim
The aim of the project is to map some of the current technologies in Smart homes, identify some of their security concerns and provide effective recommendations to overcome these.

1.1.2. Objectives
**Objective 1:** Identify and discuss the current smart home technologies available in the market using secondary and primary research methodologies.

**Objective 2:** Collect reliable data on the present availability and security features of smart homes technologies using quantitative and qualitative research methods.

**Objective 3:** Identify the security vulnerabilities of the smart home technologies through my research

**Objective 4:** Provide effective recommendations to address or minimise the explored security vulnerabilities in smart homes.
1.2. Scope

1.3. Research question

The research question for this project is provided below:

What are the current technologies available within Smart Homes and what are the security issues around this technology?

1.4. Report Structure

- The section 2 explains the secondary research conducted for the project is specified.
- The section 3 provides the approaches taken in the project is discussed.
- The section 4 provides the findings and analysis is provided is discussed.
- The section 5 provides the recommendations for end users and suppliers.
- The section 6 provides the conclusion and future work.
2.0. Literature Review

2.1. Introduction

This dissertation aims to identify key issues and challenges surrounding the use of Smart Home technologies and their security implications. Background research conducted from a wide variety of sources including relevant journals, books and other published materials on smart homes and related technologies will inform the study. This contextual research will form the literature review as a foundation to better understand the data and findings that emerge from the subsequent primary data collection. As the literature review findings may not be recent, primary research will be conducted to gather more recent information (Saunders, Lewis and Thornhill, 2016).

The concept of the Internet of things (IoT) is an important one that’s gaining currency globally. It describes how technological devices connect to each other though myriad networks and can be accessed from near and far. The internet of things was initially introduced in 1999 by Kevin Ashton. There are several applications of Internet of things which are Smart homes, wearables, Smart City, Smart grids, connected cars, connected health, smart supply chain, smart parking, smart lighting and so on. This project focusses on the smart home application of the Internet of Things.

A smart home can be said to be a home integrating a range of detectors, systems and gadgets that can be remotely accessed, monitored and controlled through a communication network (Hansen, 2010). Smart homes have existed for some time. Kitchen computer is the name of one of the first smart home devices which weighed 100 pounds (Das et al., 2002). Neiman Marcus offered it to general public in the year 1969 selling at the rate of $10,000 and it is expected the people who are using the technology must take a course in programming in order to use the system (enter and read recipes) (Bradbeer, Laurie and De Bono, 1982 p 191). Numerous versions of smart homes have ever since been developed. Examples are: MavHome, which are ordinarily also connected to the internet to give room for remote monitoring and control (Cook et al., 2003). These smart homes utilise various sensing technologies. The latest smart home appliances feature microphones for voice interaction and for the purpose of processing and storage utilises cloud. Also, they may include programming structures that makes room for the development of smart home services like Samsung’s Smarthings, Apple’s HomeKit, and Google's Weave/Brillo. These days, anyone can effortlessly be retrofitted with affordable, customized and potentially smart gadgets.

Recent study shows that the global smart home market in the year 2015 was worth $9.8 billion and is estimated to get to $43 billion by 2020 (Smart Home - worldwide | Statista Market Forecast, 2017). As stated by another study (From website august by Xfinite), the smart home market is predicted to double in the United States with the family well-being being the greatest motivator (The Safe and Smart Home: Security in the Smart Home Era, 2017). Nonetheless, the expanding deployment of internet connected gadgets in the home expose the residents to risks pertaining to privacy and security as personal details becomes remotely accessible in new ways. For example, an attacker may eavesdrop on the wireless transmission of sensors and detect activities like sleeping, showering and toileting (Srinivasan et al. 2008). Likewise, a malicious actor may remotely assume control of the home gadgets, by so doing hacking the household or launching attacks to the other domains, for instance, to overload the energy grid. Successful attacks on different commercial off the rack items have been carried out. These
attacks are not only theoretical, for example, over 73,000 video cameras were observed to be streaming their surveillance footage on the internet (Srinivasan et al. 2008).

This chapter will start by discussing the Smart home and its technologies and will focus on the security aspect of the Smart home.

2.2. Smart Home Systems
A smart home is a home, typically a new one that has unique structured wiring that allows residents to remotely control or program a variety of mechanised home electronic gadgets by inputting a single command (Jiang 2004). For instance, a property owner out of town can make use of a Touchtone phone to set up a home security system, switch gadgets on or off, control temperature gauges, program an entertainment system or home theatre, control lighting and carry out many other tasks. The field of home computerisation is growing quickly as electronic advances unite.

The home system encompasses information technologies, communications, convenience, security and entertainment. A technology called Powerline Carrier Systems (PCS) is utilised to send coded signals along a home’s current wiring to programmable outlets or switches (Usman and Sham, 2013). These signals pass on commands that correspond to addresses or locations of particular gadgets, and that control how and when those gadgets work switches (Usman and Sham, 2013). A PCS transmitter, for example, can transmit a signal along a home’s wiring, and a receiver connected to any electric outlet in the home could receive that signal and control the gadget to which it is attached switches (Usman and Sham, 2013).

One common protocol for PCS is called X10, a signaling method for remotely controlling any gadget connect to an electrical power line (Alam et al. 2012). X10 signals, which include short radio frequency (RF) bursts that represent computerized data, allow communication among transmitters and receivers (Alam et al. 2012). In Europe, technology to equip homes with smart gadgets concentrates on the advancement of the European Installation Bus, also known as Instabus (Robles et al., 2010). This implanted control protocol for computerized communication between smart gadgets comprises of a two-wire bus line installed alongside with normal electrical wiring (Robles et al., 2010). The Instabus line connects all gadgets to a decentralized communication system and operates like a telephone line over which gadgets can be controlled (Robles and Kim, 2010). The European Installation Bus Association is a part of Konnex whose major aim is to regulate home and building systems in Europe (Robles and Kim, 2010).

Echelon Corp., the maker of the LonWorks system, is assisting in driving the adoption of an open interoperability standard among merchants in the control networks industry (Chemishkian, 2002). LonWorks is an open standard for system mechanization and control for home, industrial, transportation and building markets (Ricquebourg et al., 2006). The American National Standards Institute (ANSI) has embraced the protocol hidden LonWorks control systems as an industry standard (Ricquebourg et al., 2006). The Lon Mark Interoperability Association consists of over 200 control organizations mission working on standard to incorporate multi-merchant systems in view of LonWorks networks (Ricquebourg et al., 2006).

2.3. Smart Home Software and Technology
Smart home technology was developed in 1975, when an enterprise in Scotland developed X10 (Cook et al., 2003). X10 permits compatible items to communicate with each other over a pre-existing electrical International wire of a home (Robles et al., 2010). All the devices are
receivers, and the methods of controlling the system like remote controls or keypads, are transmitters. To turn off a lamp in another room, the transmitter will transmit a message in numerical code that involves the following:

- An alert to the system that it's giving out a command,
- An identifying unit number for the gadget that should receive the command and
- A code that contains the particular command like "turn off."

All of this is planned to take place in less than a second, but X10 does have some constraints. Interacting over electrical lines is not generally dependable on the grounds that the lines get "noisy" from controlling different gadgets (Ricquebourg et al., 2006) An X10 gadget could interpret electronic interference as a command and respond, or it might not respond to the command at all. While X10 gadgets are still around, other technologies have surfaced to compete for your home networking dollar (Jiang et al., 2004).

Rather than going through the power lines, some systems utilize radio waves to interact, which is also how WiFi and cell phone signals function. Nonetheless, home automation systems do not require all the juice of a WiFi network because automation commands are short messages. The two most important radio networks in home computerisation are ZigBee and Z-Wave (Elkamchouchi and ElShafee, 2012). Both technologies are mesh networks, meaning there is more than one path for the message to get to its destination (Elkamchouchi and ElShafee, 2012).

Z-Wave utilizes a Source Routing Algorithm to decide the quickest route for messages (Mainetti, 2011). Every Z-Wave gadget is embedded with a code, and when the gadget is connected to the system, the network controller recognizes the code, decides its location and adds it to the network (Mainetti, 2011). When a command comes through, the controller makes use the algorithm to decide how the message should be sent (Mainetti, 2011). Since this routing can take up a considerable measure of memory on a network, Z-Wave has built up a hierarchy between gadgets: Some controllers start messages, and some are "slaves," which implies they can only convey and react to messages (Mainetti, 2011).

ZigBee's name show the mesh networking idea since messages from the transmitter zigzag like bees, searching for the best path to the receiver (Osipov, 2008). While Z-Wave utilises a restrictive technology for operating its system, ZigBee's platform depends on the standard set by the Institute for Electrical and Electronics Engineers (IEEE) for wireless personal networks (Han and Lim, 2010). This implies any organization can build a ZigBee-compatible product without paying licensing charges for the technology behind it, which may inevitably give ZigBee a favourable position in the marketplace (Han and Lim, 2010). Like Z-Wave, ZigBee has fully functional gadgets (or those that route the message) and reduced function gadgets (or those that do not) (Han and Lim, 2010).

Making use of a wireless network give more flexibility for placing gadgets, but like electrical lines, they might have intrusion. Insteon provides a way for your home network to relate over both electrical wires and radio waves, making it a two-way mesh network (Kim et al., 2012). If the message is not getting through on one platform, it will attempt the other. Rather than routing the message, an Insteon gadget will broadcast the message, and all gadgets pick up the message and broadcast it until the command is carried out (Kim et al., 2012). The gadgets act like peers, as opposed to one serving as an instigator and another as a receptor. This implies
that the more Insteon gadgets that are installed on a network, the stronger the message will be (Kim et al., 2012).

2.4. Setting Up a Smart Home
X10, Insteon, ZigBee and Z-Wave simply give the technology for smart home communication. Manufacturers have made associations with these systems to make the items that utilise the technology (Robles et al., 2010). Below are some examples of smart home products and their uses.

- Cameras will track your home's exterior regardless of the possibility of it's pitch-black outside.
- Plug your tabletop light into a dimmer rather than the wall socket, and you can light up and dim by simply pressing a button.
- A video door phone gives more than a doorbell; you get a picture of who's at the door.
- Motion detectors will send an alert when there's motion around your house, and they can even differentiate among pets and criminals.
- Door handles can open with scanned fingerprints or a four-digit code, removing the need to fumble for house keys.
- Audio systems share the music from your stereo to any room with connected speakers.
- Channel modulators take any video signal - from a security camera to your favorite television station -- and make it possible to view on every television in the house.
- Remote controls, keypads and tabletop controllers are the methods of activating the smart home applications. Gadgets also come with built-in web servers that permit you to access their data via web.

The keypad will transmit message to your lamp. These items are accessible at home improvement stores, electronics stores, from technicians or online. Before purchasing, confirm that the technology is associated with the product. Products using similar technology should work together regardless of different manufacturers, but joining up an X10 and a Z-Wave product needs a bridging gadget (Robles et al., 2010).

In planning a smart home can be for a little home automation or the entire home system integration. You could start with a lighting starter pack and add on security gadgets later. If you want to begin with a bigger system, it’s a good idea to carefully plan how the home will work, especially if rewiring or renovation will be needed. Furthermore, you'll want to strategically place the nodes of the wireless networks in order to have a good routing range. The cost of a smart home differs depending on how smart the home is. To gradually build a smart home, starting with a basic lighting system, it might just be a few hundreds of dollars. A more modern system will be tens of thousands of dollars, and elements of home theatre systems increase the cost of a system about 50 percent (Robles et al., 2010).

2.5. Advantages of Smart Home

Smart homes clearly have the capacity to make life easier and more convenient. Home networking can likewise give peace of mind (Lutolf, 1992). Whether you’re at work or on vacation, the smart home will notify you to what is happening, and security systems can be built to give an immense amount of help in an emergency. For instance, not only would a
resident be woken with alert of a fire alarm, the smart home would likewise unlock doors, call the fire department and light the way to safety (SURYADEVARA, 2016).

Smart homes likewise give some energy efficiency savings. Because systems like Z-Wave and ZigBee put some gadgets at a reduced functionality level, they can go to sleep and wake up when commands are issued (Briere and Hurley., 2013). Electric bills go down when lights are automatically turned off when a person leaves the room, and rooms can be heated or cooled depending on the person that is there at any given moment. One smart homeowner boasted her heating bill was about one third less than a same sized normal home. Some gadgets can track how much energy each appliance is using and command it to use less (Lutolf, 1992).

Smart home technology guarantees tremendous benefits for an elderly person living alone. Smart homes could alert the occupant when it was time to take medicine, notify the hospital if the occupant fell and track how much the resident was eating. If the elderly person was a little forgetful, the smart home would carry out tasks like shutting off the water before a tub overflowed or turning off the oven if the cook had wandered away. It also permits adult children who might live elsewhere to participate in the care of their aging parent. Easy-to-control computerized systems would give similar benefits to those with disabilities or a limited range of movement (Lutolf, 1992).

2.6. Smart Home Security
Traditional security systems protect homeowners, and their property from intruders. A smart home security system, nonetheless, offers numerous advantages (Gomez, and Paradells, 2010). Home automation technology alerts homeowners of any problems, so that they can investigate. Artificial intelligence programs monitor the homeowner's routines, and other vital information. Also, alerts emergency personnel when necessary (Gill et al., 2009).

2.6.1. Smart Home Fire Protection
Smart home security system provides much more protection than the regular fire alarm. This sort of system checks carbon monoxide levels and in addition looking out for signs of fire and monitors every area of the home. In case of a fire outbreak, the smart home security system can notify the homeowner and alert emergency services. Artificial intelligence programs are even capable of pointing out the location of the fire, and give that information to fire department personnel as they respond (Lee and Lee, 2004).

2.6.2. Access Control
Security codes, motion sensors, and cameras provide data to a smart home security system, permitting it to decide if an individual is a resident, a cleared visitor, or an intruder. Motion sensors trigger a notification, allowing the artificial intelligence program realize that there is someone or something to be analysed. Software for facial recognition and security codes permits the security system to allow residents into the home, while based on preprogramed data restrict access to other people (Kim et al., 2012).

Anytime smart home security system identifies an unknown person, it can make the video of the visitor available to the homeowner. Guests that are welcome can be given clearance and permitted into the house remotely. Unwelcome guests can be ignored, and people trying to break in will trigger a call to the police (Kim et al., 2012).
2.6.3. Artificial Intelligence Programs Protect the Home owner

Thieves and robbers are the major problem in a normal home. However, in Smart homes cameras, motion sensors and other detection mechanisms are used to detect the unwanted movements. Besides, there is an individual movement detection that can be used to locate any threats for individuals outside the home. However, the individual movement detection can be confusing at some times when an individual has a different action that what is expected. This can cause unwanted emergency alerts. However, the motion detection of the smart home technology is very much useful for elderly people or people who need support (Reinisch et al., 2010).

2.7. Technology and Research in Smart Home Security

Many smart home gadgets provide home automation technology, yet the smart home security system provides many advantages that can guarantee the well-being of the property owner. In this section, we analyse the tools related to Smart Home Security.

2.7.1. Smart Home Networks User Verification Using Neural Network

The network user verification scheme has two stages: the user registration stage and user verification stage (Reyhani and Mahdavi, 2007). First, authorised users have to register in the verification system by providing their username and password. In second stage, that is, the user verification stage, the system approves the authenticity of the users. In the user registration stage, the system administrator obtains the training designs from user names and passwords to train the neural network. The registration process is described below (Reyhani and Mahdavi, 2007):

- Every user selects an appropriate username and password and hand into the system administrator.
- The system uses a one-way hash function to the user name and password and the result is used as the training design. So, the training pattern comprises of hashed user name, as the contribution of the neural network, and the corresponding hashed password, as the desired output of the neural network.
- Before preparing the neural network, it is necessary for the system to normalize the ASCII codes of the characters of the patterns of training.
- The system administrator utilises these training patterns for training the RBF network. Following the training process, the system administrator keeps the RBF network weights in the system.

In the user authentication stage, the authentication system utilises the trained RBF network and uses a similar one-way hash function to confirm the legality of the users. The process of authentication is described below (Reyhani and Mahdavi, 2007):

1. The system utilises a similar hash function on the inputted username and password.
2. The system pulls out an output through the trained neural network.
3. The system compares the result of the RBF network with the hashed password. If the results are equal, the user is identified as an authorized user, or else, the user is rejected as a fraudulent user.

2.7.2. Sentry@Home

Smart Home environments normally are equipped with various types of detectors and tracking devices for context-aware service provisioning. Besides, individuals want to exploit the comfort
and added value of customized context-aware services. Privacy and traceability becomes a grave concern on the other hand. The question of how trust cannot be built into inherently untrusted services in a potentially unfriendly environment arises. What is the assurance that in the end all sensitive information is deleted or safely kept? The Sentry@HOME concept, as part of our User-centric Privacy Framework, tackles these concerns (Bagüés et al., 2007).

Sentry@HOME is intended to become an essential part of the user’s home environment; absolutely embedded into the Smart Home software infrastructure. The Smart Home itself then can be leveraged to act as a privacy proxy for a tracked person. On the user’s behalf, it constitutes the central privacy implementation point for all privacy relevant accesses to private or sensitive information. We are self-assured that our input, the combination of Smart Homes and a privacy-aware framework, significantly adds to the success of customized pervasive computing systems (Robles et al., 2010).

2.7.3. Defending DDoS Attacks Caused by Spam

Distributed Denial of Service (DDoS) attack is an extensive, coordinated attack on the availability of services at a victim system or network resource (Alomari et al., 2012). DDoS attack through spam mail is one of the recent kind of common DDoS attack. In this type, the attacker infiltrates the network by a small program connected to the spam mail. After the execution of the file attached, mass mails from other machines in the domain eats up the mail server resources and the result is denial of services (Robles et al., 2010).

This defence mechanism is a multi-layer method to defend the DDoS attack caused by spam mails. This method was carried out in the mail system and monitored the results. The result shows that our method is very effective. The method has six layers. This method is a mix of adjusting source filters, content filters, general email policies, network monitoring policy, educating the user & timely reasonable solutions of the network administrator. Adjusting the source filters reject the incoming connections before the delivery of the spam mail. The content filters evaluate the contents of the mails and blocks the incoming unwanted mails. Network monitoring method gives general solution to recognise the attacks prior to the attack and also during the attack. Business houses should educate the user about prospective attack occasions and reacting ways to stop it. The reasonable solutions of the network administrator play a significant role during the attack period and even post attack period. The combination of these layers gives best strategy to stop the DDoS attacks established through spam mails (Robles et al., 2010).

2.8. Conclusion

A Smart Home is a residence that utilises a Home Controller to incorporate the occupant’s different home automation systems. The most well-known Home Controllers are those that are connected to a Windows based PC during programming only, and are thereafter left to carry out the home control functions on a stand-alone basis. Integrating the home systems permits them to inter-relate with one another through the home controller, thereby allowing single button and voice control of the different home concurrently, in pre-programmed occasions or operating modes. Security has been a significant issue in the smart home applications. In the secondary research the background study about the smart home, the technologies used in the smart homes such as X10 gadgets, Z-Wave, ZigBee, and Insteon gadget, how the smart home can be set up in a home, and advantages of the smart home. Moreover,
the smart home securities such as fire protection, access control, and artificial intelligent programs are discussed.
3.0. Methodology

3.1. Secondary Research

The secondary research undertaken for the literature review was carried out using information gotten from books, journals and articles among other electronic and non-electronic sources from Cardiff Metropolitan University. Other electronic sources used in writing the review were IEEE materials and also direct science accessible through the University. I also got several research papers that formed the basis of the literature review from my supervisor.

3.2. Primary research

This investigation into the Security challenges and implications surrounding Smart Home technologies uses a mixed methodology in collecting, analysing and integrating qualitative and quantitative research data to inform the findings.

The table XX provides the advantages and disadvantages of utilising mixed methodology for the project

<table>
<thead>
<tr>
<th>Table 1: Advantages and disadvantages of mixed methodology (Tashakkori and Teddlie, 1998)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advantages of Mixed Methodology</strong></td>
</tr>
<tr>
<td>• It strengthens and counterbalances the weakness of both qualitative and quantitative research for this project.</td>
</tr>
<tr>
<td>• It gives a thorough and an all-inclusive viewpoint of the research problem than either qualitative or quantitative approaches alone.</td>
</tr>
<tr>
<td>• It gives an avenue for developing better and more context definite instruments.</td>
</tr>
<tr>
<td>• It aids in illustrating findings or how causal strategy works.</td>
</tr>
</tbody>
</table>

Quantitative research is a methodical investigation achieved using statistics, mathematical or computational approach (Kenner, Busch and Kenner, 1979). Quantitative research essentially utilises questionnaires in gathering information and producing the results by some specific analysis for example, mathematical models. In this project the online survey will be created to collect quantitative data. Furthermore, qualitative method involves the studied use, compilation and selection of materials that are verifiable such as case study, personal experience, observations, interviews, etc. (Willig 2008). It is also stated as fact-based research where the information is not in number-like in form (Willig 2008). In this project the interview is used to collect qualitative data. Both the qualitative and quantitative analysis are involved in this project. Identifying the advantages and disadvantages of qualitative and quantitative research method will assist in maximising the finding on the security challenges and implications surrounding Smart Home technologies. Find critical analysis as provided in table XX:
Table 2: The critical assessment of qualitative and quantitative research methods

<table>
<thead>
<tr>
<th>Advantages of Qualitative Research</th>
<th>Disadvantages of Qualitative Research</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualitative research is crucial in the starting of a study when the researcher might be considering the area of concentration for the research. This kind of investigation does not require a strict blueprint of action before it begins. This provides the pro a chance to develop the study more truly. An additional basis of choosing qualitative research is the master procures divided and rich data as broad made demonstrations or visual assertion, such as, photographs. This kind of investigation looks at setting and social significance and its effects on people, which is of value especially in the humanistic structure.</td>
<td>The investigator of a study that makes use of qualitative research is enthusiastically added straight away, which makes the master a subjective view of the study and its people. The pro describes the examination in relation to his or her own definite unequal view, which skews the data collected. Another disadvantage is that this technique of inspection is to a great extent boring and can continue going for an significant duration or even years (Woolf, Tanna, and Karam Singh, 1985).</td>
</tr>
<tr>
<td>Quantitative research permits the researcher to analyse and research information. The relationship between a free and ward variable is seen in a straightforward part. This is crucial in view of the fact that the focus of the expert is results of the examination (Miles and Huberman, 1994). Besides, it is useful in testing predictions in examinations as after result of its ability to evaluation data using bits of knowledge (Miles and Huberman, 1994).</td>
<td>The essential weight of quantitative survey is the setting of the study or examination is left (Miles and Huberman, 1994). Furthermore, it does not break down things in a trademark setting or discuss the enormity of things for distinguishing people as subjective examination does (Miles and Huberman, 1994). Another stumbling block is that an immense description of the masses must be examined; the greater the example of individuals examined, the more really definite the results will be (Miles and Huberman, 1994).</td>
</tr>
</tbody>
</table>

3.2.1. Selection of participants in the survey
The demographic for quantitative and qualitative research will be the general public who use smart home technologies above age 18 who works in technology industry and people who installed smart home technology in their home. The major reason for selecting the specific group of people is because that the project focus on getting the security issues of using smart home technology which needs personal experience with smart home technology or have a IT background to find the security issues. The demographic for this research will be the general public who use smart home technologies above age 18 who works in technology industry and people who installed smart home technology in their home. The survey will be openly administrated online and available globally. The interview will be with a selective number of interviewers based in the UK. All the primary data collection will be undertaken between January to February 2017 due to the time restriction. From a combination of analysis of primary and secondary data collected will draw out the trends and recommendation to address the research question.
3.2.1. Approaches used for the research
Interviews were used for qualitative research gathering while questionnaires (online surveys) were used for quantitative research. The critical assessment of each methodology will help to focus more on the different responses as given in the table XX. face-to-face interviews will receive comprehensive explanation and attitude about the security of smart homes technologies. Likewise, online survey will bring abstract data from many people around the world.

Table 3: Critical assessment of each method used

<table>
<thead>
<tr>
<th>Survey methodologies</th>
<th>Positive reasons</th>
<th>Negative reasons</th>
</tr>
</thead>
</table>
| Personal interview   | • It has the capacity to target a particular groups of people  
                      | • Provides higher rates of response  
                      | • This gives room for respondents’ attitude to be observed | • its times consuming  
                      | • sometimes it is not cost effective |
| Online survey        | • Easily understood because they are the commonest survey method used  
                      | • The responses received from the survey can be easily evaluated  
                      | • It allows respondents to have the liberty to easily express their personal view.  
                      | • it gives room for quicker and effective responses  
                      | • it is Cost effective  
                      | • easier to carry out  
                      | • in comparison with other methods of collecting information, it requires lesser time to develop  
                      | • geographical dependence can be reduced or avoided since it is conducted remotely  
                      | • With survey software, advanced statistical proficiency can be utilized to analyse survey information to confirm reliability, validity and statistical significance which includes the ability to analyses multiple variables | • It is one sided and has only about 7 options for choice. Thus, It may most likely not capture the correct attitudes of the respondent.  
                      | • Respondents may not be inspired to provide correct and honest answers  
                      | • Respondents may not feel at ease to give responses that present themselves in an unfavourable manner.  
                      | • Respondents may not be totally aware of their reasons for any answer given as a result of insufficient memory on the subject, or even boredom.  
                      | • The rate of validity on closed-ended questions may be lower compared to other types of question.  
                      | • There may be cases of data errors resulting from non-responses to question. Bias may be created as the number of respondents that responds to a survey question may be different from those who decide not to respond.  
                      | • Options for answer to survey question could result to unclear information because respondents may interpret answer options differently. For example, the answer option “quite agree” may mean different things to different subjects, and have its own meaning to  
                      |
Survey methodologies | Positive reasons | Negative reasons
--- | --- | ---
| | | every individual respondent. Answers for ‘Yes’ or ‘no’ options can also be tricky. The response of respondents’ may be “no” if there is no provision for the option “only once”.
| | | Customised surveys stand the risk of having some types of errors

The interview questions used are given in appendix XX and the questionnaires or survey utilised are shown in appendix XX.

3.2.3. Method Used in Collecting Information

The interview was done using face-to-face, Skype, and by telephone calls. See reasons for selecting these interview mediums in table XX. Different interview methods are used in the project in order to receive wide range of responses. By and large, interview will not scope many responses due to lack of time, hence, in this project various types of methods of interviews were introduced to increase the time to get more responses with regard to the security of smart homes.

Table 4: Reasons for selecting these mediums for the interview

<table>
<thead>
<tr>
<th>Medium used for the interview</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td>A lot of people can be reached through this method. Almost everybody can easily access a telephone. This is a useful method in a case whereby respondents are not close by.</td>
</tr>
<tr>
<td>Skype</td>
<td>This is a semi-formal method used for long distance survey. It is reliable and through this medium enough responses can be achieved. It saves time and cost and also gives room for respondents to be observes</td>
</tr>
<tr>
<td>Email</td>
<td>With this method, more people can be involved and respondents have the liberty to respond at their own convenient time.</td>
</tr>
</tbody>
</table>

The survey includes different types of questions which are single selection, multiple selection, and descriptive answers. the survey questions are published online using google forms as well as personal handout were given out. See table XX for the reason for selecting these methods to gather responses for the survey.

Table 5: The reason for selecting these methods to gather responses for the survey

<table>
<thead>
<tr>
<th>Medium used for questionnaires / survey</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publishing on the internet</td>
<td>It is a remote way of gathering data. It is an easy way to get comments from different countries.</td>
</tr>
</tbody>
</table>
### Medium used for questionnaires / survey

<table>
<thead>
<tr>
<th>Medium used for questionnaires / survey</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hand to hand distribution in UK (handout)</td>
<td>This way, more responses can be gotten. Besides, this will ensure that all categories of individuals are captured in the survey.</td>
</tr>
</tbody>
</table>

The survey links will be shared using social medias such as whatsapp, viber, facebook, twitter, and gooogle+ (See evidence in appendix XX).

#### 3.2.4. Survey Questions types

Open-ended questions and closed-ended questions are the two most common types of questions used in the survey. There are no predefined options in open-ended questions. Participants provide their own answers. Closed-ended questions on the other hand restricts answers of participants to response options contained in the questionnaire (Lavrakas, 2008). Table XX (Lavrakas, 2008) shows the critical analysis of open-ended questions and closed-ended questions

*Table 6: Critical Analysis on open-ended and Closed-ended questions (Lavrakas, 2008)*

<table>
<thead>
<tr>
<th></th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Open-Ended Questions</strong></td>
<td>Respondents are allowed to respond to questions the way they want and their response is precise.</td>
<td>It consumes time and sometimes responses are ambiguous.</td>
</tr>
<tr>
<td><strong>Closed-Ended Questions</strong></td>
<td>It is time efficient and also responses are unambiguous.</td>
<td>Some answer options do not clearly indicate the particular answer of respondents.</td>
</tr>
</tbody>
</table>

#### 3.3. Survey and Interview Analysis

The interview was analysed using responses received from the response groups such as people who uses Smart Home technology in their houses and the people who have IT background. Then the collected responses from the interview will be go through the following steps (Saunders, Lewis and Thornhill, 2016):

- Step 1: Summarisation
- Step 2: Grouping
- Step 3: Structuring

Moreover, the online survey results were exported to Excel for advanced analysis. However, the major analysis was done by the survey engine converting and visualising data into graphs and diagrams. The automatically generated graphs for responses received for each question in the survey will give the basic understanding of the types of answers received by the individuals. Also, the online survey engine provides the free and easy distribution and accessibility to the survey questions. Survey engine allow the author to share the links through email and other
social media platforms and it also allow the people to response without signing in to the link. This free distribution and accessibility allowed the many individuals to given responses.

### 3.4. Questions used for Interview and survey

The purpose for selecting the questions for interview and survey is shown in table XX

<table>
<thead>
<tr>
<th>Interview and survey questions</th>
<th>Reasons for the questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Background questions</strong></td>
<td></td>
</tr>
<tr>
<td>Select your age group?</td>
<td>This is to get background information on the respondent.</td>
</tr>
<tr>
<td>Select your country of residence?</td>
<td>This is to get background information on the respondent.</td>
</tr>
<tr>
<td>Gender</td>
<td>This is to get background information on the respondent.</td>
</tr>
<tr>
<td>What kind of home do you currently live in?</td>
<td>This is to get background information on the respondent.</td>
</tr>
<tr>
<td>Do you work in a technology firm, if so which one?</td>
<td>This is to get a background information on the respondent. This will give an idea whether person has extra technical knowledge or is a basic Smart home user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Smart Home Experience</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of smart technologies do you have installed in your home?</td>
<td>This is to confirm whether the respondent is personally using smart home technologies</td>
</tr>
<tr>
<td>What type of technologies did you install in your smart home?</td>
<td>To get an understanding about the technology been used in the house</td>
</tr>
<tr>
<td>If you had to choose one form of smart home technology to be implemented or installed across homes in your country of residence, which would you choose from the following list?</td>
<td>To gather people’s views with respect to smart home technologies and their popularity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prioritise with respect to Smart Homes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Which factors did you (or would you) consider as important when installing smart home technologies in your home?</td>
<td>To identify respondents’ views on the important factors that drive their choices regarding smart home technologies.</td>
</tr>
<tr>
<td>What was the key reason you installed the Smart home technology?</td>
<td>This is an open-ended question which allow the respondent to provide a detail explanation regarding the reason for the smart home installation in their home.</td>
</tr>
<tr>
<td>Do you think the smart home technology was value for money?</td>
<td>To get an overall idea whether people are happy about the technologies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security issues faced from Smart Home technologies</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you aware of the security features of your smart home technology?</td>
<td>To get an idea whether people have idea about the entire security features of the technologies they use.</td>
</tr>
<tr>
<td>If yes (for above question) can you list them?</td>
<td>Allow people list their known security features of the system.</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Do you have any security concerns around your smart home technology?</td>
<td>Gather information regarding their security concerns.</td>
</tr>
</tbody>
</table>

### Recommendations to reduce the security issues

<table>
<thead>
<tr>
<th>What do you advise the user to do in order to keep their smart home safe?</th>
<th>Collect recommendations for the security issues.</th>
</tr>
</thead>
</table>

### 3.5. Steps taken to arrive at the recommendation

Secondary research was initially carried out and primary research was then conducted. The primary research will undergo **statistical analysis and graphical presentation**. However, the secondary research findings will be done by self-check questions, suitability to the aim and objective of the project, benefits of the information collected will be considered and the **content filtering approach** to get the major points mentioned (Saunders, Lewis and Thornhill, 2016). The **comparison method or approach** was used to compare and contrast the answers gotten from the secondary results and primary results. From the critical analysis, the most appropriate recommendations will be gotten. Thus, in summary, this project uses **hybrid or mixed method** approach to arrive at the recommendations.
4.0. Findings and Analysis

4.1. Introduction

This chapter primarily focuses on analysing the responses received from the interviews and survey undertaken as part of this research. In total 20 responses were received for interviews and 102 responses were received for the online survey. There are several methods were used to analyse the interview and survey responses which are statistical analysis, graphical analysis, content filtering approach, and comparison method. The graphical representation was mainly used in survey analysis. The summary of the responses is provided in the sub sections below.

4.2. Interview Analysis

The summary of the interview findings is provided below:

40% of respondents stated that they had smart home devices installed in their homes. Moreover, the types of devices they already had installed included and ranged widely from: keyless connection, Logi Circle, Thermostat, Smoke detector, Smart Tvs, Smart lighting, Smart Multimedia, Smart Refrigerator, iKettle, Weather Station, and Security System. It is also identified that 30% of respondents interviewed thought that security systems should be installed across homes in their country of residence, 10% thought it should be Thermostat, 5% thought it should be smoke detector while the remaining 5% think it should be keyless connection.

While some of the respondents interviewed thought that smart home technology was easy to use since they can have access to monitoring and controlling their homes where ever they are through their mobile phone apps or through online portals, some others think that they are user friendly; operating smart home devices are not complex. Some respondents feel that such devices are reliable; for devices, such as thermostats, they regulate themselves whether or not there is anybody at home. To some respondents, they are affordable. There are many Smart Home technology companies, hence, the services are affordable due to competition amongst the technology companies.

The main reason, more than 50% of the interviewed respondents gave for installing Smart technologies in their homes was for added security. around 20% of the people, they simply wanted to modernise the security features in their homes while the other 30%, they opted for smart home technologies because they are easy to use.

More than 60% of the respondents totally agree that smart home technologies give them value for their money. less than 20% of the respondents were not sure whether or not they received value for money for installation of smart home technology in their homes. Almost 30% of the respondent think they are too expensive and the service does not equal the amounts paid to acquire the technology (For example, it was stated that most of the smart home technologies does not provide instalment payment and taking a loan to buy it is not worth for its use, and also it was stated that smart home technologies are for rich category of people whose income is 6 digits). More than 75% of the respondents interviewed, especially those within the age brackets of 18 to 60 were aware of the features of their Smart Home technologies installed in their homes and less than 5% of the respondents were not aware of the features. Some of the features specified are Devices are remotely controlled through the use of mobile phone apps or online portals, devices are dependable since they need minimal physical control, they are easy to use, and they think and act on behalf of the users that is why they are tagged smart devices.
The 40% of respondents interviewed stated that they had concerns around their smart home technology. More than 75% of them thought that since the control of such devices is internet related, they fear, the system can be hacked or infiltrated, hence, they could have security issues or a mishap as a result of infiltration of devices. 25% of others are completely unaware of any security issue with their devices, rather, they are enjoying them since the devices make life a lot easier for them.

The respondents of the interview specified some suggestions provided to avoid security breach in their home which are:

- Use complete passphrases,
- Do not use public Wi-Fi,
- Do not use default username and passwords for devices,
- Install malwares for devices,
- Do not allow untrusted people have access to your devices

4.3. Survey Analysis

The responses received for the survey questions are presented using bar chart and pie chart. This provides a clear visual representation of the responses received and it assist in summarising the findings. The visual representation and the explanation for each question are provided below:

4.3.1. Personal Information

Question 1: Select your age group?

![Pie chart showing age distribution]

Respondents’ age bracket as seen in the survey ranged as follows: almost 52.9% of the survey respondents are the age between 18 to 30 years, while 26.5% of the respondents are between the age 30 and 50 and 15.7% of the respondents are between the age 50 and 70.

Question 2: Select your country of residence?
Survey respondents resided primarily in the UK with 59.8%, the US made up 22.5%, Saudi Arabia was 11.8% while other countries made up the remaining part of survey respondents.

**Question 3: Gender**

Males constituted 59.8%, whilst females made up 40.2% of the total survey respondents.

**Question 4: What kind of home do you currently live in?**

In terms of the kind of home respondents lived in, a house was 31.4%, a shared house was 41.2% and a flat was 26.5%.

**Question 5: Do you work in a technology firm, if so which one?**
More than 50% of the respondents do not work in a technology firm while some work with technology firms like Home security system, Samsung Smart things, August Smart Lock, IBM, Whirlpool, LG, Panasonic, HP, Acer, Infosys, Microsoft, Laxaflex, Netatmo and Dell.

4.3.2. Smart Home Experience

Question 6: Do you have Smart Home technology installed in your home?

88.2% of the total respondents had Smart home technology installed in their homes.

Question 7: What type of smart technologies do you have installed in your home?

The following are statistics of smart home technologies installed in homes:

- Smoke detector: 87.3%
- Thermostat: 81.4%
- Security system: 61.8%
- Weather station: 26.5%
- iKettle: 34.3%
- Logi Circle: 33.3%
- Keyless connection: 72.5%
- Others: 37.3%
4.3.3. Priorities with respect to Smart Home Technologies

Question 8: Which factors did you (or would you) consider as important when installing smart home technologies in your home?

![Chart showing factors considered for smart home technology installation]

Figure 8: Survey question 8 Analysis

The following statistics illustrate factors that were considered for the installation of smart home technology in the home:

- 85.3% of respondents stated they make their choice based on the technology's user friendliness,
- 86.3% said because they are useful,
- 86.3% say they are reliable,
- 78.4% say because of prices,
- 72.5% say because of maintenance while 15.7% respondents have other reasons.

Question 9: What was the key reason you installed the Smart home technology?

![Chart showing reasons for installing smart home technology]

Figure 9: Survey question 9 Analysis

The reason for installing smart home technology in the houses are for;
- more than 85.3% of people mentioned ‘security’
- 83.3% of people mentioned ‘for ease of use’.

Question 10: Do you think the smart home technology was value for money?

![Pie chart showing responses to the survey question]

Figure 10: Survey question 10 Analysis

82.4% of the total respondents for this survey are of the opinion that smart home technology
gives them value for their money. 14.7% are not sure whether or not they derive any value for the smart home technology they have in their homes.

4.3.4. Security issues faced from Smart Home technologies

Question 11: Are you aware of the security features of your smart home technology?

![Survey question 11 Analysis](image1)

81.4% are aware of the features of the smart home technology installed in their homes, while 16.7% are not sure.

Question 12: If yes (for above question) can you list them?

![Survey question 12 Analysis](image2)

The following are itemised summary of responses of features of home technology installed in their homes.

i. monitoring and control of smart home technology can be done via mobile phone app
ii. control is easy
iii. control of home devices are done remotely
iv. the devices relieve stress
v. they take care of things on behalf of their owners
vi. thermostat for example, regulates itself when there's nobody at home
vii. online portals and apps help control devices
viii. some are not sure
Question 13: Do you have any security concerns around your smart home technology?

**Figure 13: Survey question 13 Analysis**

Most of the people are concerned about the security of the smart home technology. Because most of them believe that the use of internet will increase the risk of data loss or any other types of attacks.

4.3.5. Recommendations to reduce the security issues

Question 15: What do you advise the user to do in order to keep their smart home safe?

**Figure 14: Survey question 14 Analysis**

They following advice was suggested by respondents

i. installation of malware protection
ii. use of multifactor authentication
iii. avoiding the use of public Wi-fi
iv. keeping devices away from untrusted people
v. changing default admin user names and passwords.
vi. always ensure that devices are up to date
vii. always monitor the devices and alert the appropriate agents in case of any suspicious
activities.

vii. always be careful and vigilant

viii. never use network provider for home devices with main computer

ix. use only known devices

x. use software and hardware firewalls

xi. always research about a brand before purchasing. Ensure the brand of smart home device about to be purchased has gotten it is security right

xii. use cloud services

xiii. minimize the number of smart home devices. The more devices connected online, the more users are exposed to cyberattacks.
5.0. Recommendation

5.1. Introduction

The recommendations in this chapter are mainly derived from the primary and secondary research regarding how to avoid security issues or challenges. The recommendations are not just for the end users of the technologies but also for manufactures or producers of the technologies. The recommendations are categorised into different factors within the Smart Home technologies which are web interface, authentication, transport encryption, privacy, mobile interface and physical security.

5.2. Recommendation for Manufacturers

The table 11 provides a detail list of ways in which the manufacturers or producers of the Smart home technology can reduce the security threats faced.

Table 8: Recommendation list for Smart Home technology manufacture

<table>
<thead>
<tr>
<th>Category</th>
<th>Smart Home Technology Security Consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Interface</td>
<td>• The manufacturer should ensure that the weak password should not be allowed in the Smart Home web interface.</td>
</tr>
<tr>
<td></td>
<td>• The manufacturer should ensure that the account lockout mechanism should be implemented in the Smart Home web interface.</td>
</tr>
<tr>
<td></td>
<td>• The manufacturer should ensure that at least the XSS, SQLi and SSL vulnerabilities should be testing before the release of the Smart Home technology.</td>
</tr>
<tr>
<td></td>
<td>• The manufacturer should ensure that the Smart home technology web interfaces are mainly using HTTPS protocol to ensure secure data transmission.</td>
</tr>
<tr>
<td></td>
<td>• The manufacturer should ensure that the Smart Home technology interface should have the force protocol to prompt the end user to change the default password in their first use.</td>
</tr>
<tr>
<td></td>
<td>• The Manufacturer should ensure that the web interfaces of the Smart Home technology should have the active and updated firewall protection.</td>
</tr>
<tr>
<td>Authorisation protocol or</td>
<td>• The manufacturer should ensure that the web interface of the smart home technology should allow only strong password selection.</td>
</tr>
<tr>
<td>authentication protocol</td>
<td>• The manufacturer should implement at least two level authentications to the smart home technology to guarantee the safety.</td>
</tr>
<tr>
<td></td>
<td>• The manufacturer should allow the ensure of the system to specify the expiry date of the password created. But by default, it should be for a month period.</td>
</tr>
<tr>
<td></td>
<td>• The manufacturer should implement the password reset procedure more secured by implementing secure...</td>
</tr>
<tr>
<td>Authentication Protocols</td>
<td>The manufacturer should allow the smart home technology to divide and group the end users into multi user environment.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Transport Encryption</td>
<td>The Manufacturer should ensure that the web interfaces of the Smart Home technology should have the active and updated firewall protection. The manufacturer to assure that the Newest version of SSL/TLS technology is used in the implementation of the smart home technology. The manufacturer should implement the secured encryption and decryption protocols should be implemented to secure the data in the smart home. The manufacturer should implement the communication between the devices within the smart home technology are encrypted and secure ways to decrypt the message in the receiving end.</td>
</tr>
<tr>
<td>Privacy</td>
<td>The manufacturer should ensure that only the essential data regarding the customer should be collected and stored. The manufacturer should confirm that the collected data from the customers should be stored securely. The manufacturer should monitor that the data retention policy is designed and practiced in the company. The manufacturer should collect less sensitive data from their customers. The manufacturer should open the door for their customers to ask questions and view their personal details stored in the company. Also, they should have the right to request the company to delete the data.</td>
</tr>
<tr>
<td>Mobile Interface</td>
<td>The manufacturer Confirm the use of transport encryption. The manufacturer should ensure that the web interface of the smart home technology should allow only strong password selection. The manufacturer should implement at least two level authentications to the smart home technology to guarantee the safety.</td>
</tr>
<tr>
<td>Physical Security</td>
<td>The manufacturer should ensure that the hardware is protected with the minimum number of USB ports or other external ports. The manufacturer should ensure that the Smart Home technology is tamper resistant.</td>
</tr>
</tbody>
</table>
5.3. Recommendation for end users
The recommendations for Smart Home technology end users are given in table X2.

Table 9: Recommendation for Smart home technology end users.

<table>
<thead>
<tr>
<th>Category</th>
<th>Smart Home Technology Security Consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Interface</td>
<td>• The end user of Smart home technology to make sure that they use the HTTPS to browse online on the web browsers.</td>
</tr>
<tr>
<td></td>
<td>• The end user of Smart Home technologies should ensure the usage of two level authentications in the web interface. Confirm the use of two factor authentications for web interface</td>
</tr>
<tr>
<td></td>
<td>• The end user should ensure that the firewalls are up to date and it is active</td>
</tr>
<tr>
<td></td>
<td>• The end user should change the default password when he or she try to use the system.</td>
</tr>
<tr>
<td></td>
<td>• The end user should not disable the lockout functionalities of the web interface.</td>
</tr>
<tr>
<td></td>
<td>• The end user should specify a short password expiry mechanism in the web interface.</td>
</tr>
<tr>
<td></td>
<td>• The end user should specify the change the default user name and password in the interface for the smart home technologies.</td>
</tr>
<tr>
<td>Authorisation protocol or</td>
<td>• The end user should change the device default username and password.</td>
</tr>
<tr>
<td>Authentication protocol</td>
<td>• The end user should change the password expiry days to less than 30 days to ensure the security.</td>
</tr>
<tr>
<td></td>
<td>• The end user should provide limited access privileges to all the users and few and transited users should have the maximum access privileges.</td>
</tr>
<tr>
<td></td>
<td>• The end user should assure that all the users of the smart home technology should make use of their two level authentications.</td>
</tr>
<tr>
<td>Transport Encryption</td>
<td>• The end user should ensure the use of HTTPS for any web related transactions to assure safety.</td>
</tr>
<tr>
<td>Privacy</td>
<td>• The end user should not store sensitive and personal information in to the mobile device which is linked to the smart home network.</td>
</tr>
<tr>
<td>Mobile Interface</td>
<td>• The end user should make use of mobile PIN for extra security in the smart home.</td>
</tr>
<tr>
<td></td>
<td>• The end user should always confirm the use of two level authentications.</td>
</tr>
</tbody>
</table>
| Physical Security | • The end user should ensure to specify some short days for the password expiry.  
• The end users should not install the unauthorised mobile applications in the device. |

### 6.0. Conclusion and Future works

From the primary and secondary research conducted it is confirmed that the use of Smart Home technologies is increasing drastically, which will trigger increased security implications. From the research, it is identified that there is research conducted to identify and provide recommendation for the IoT application but however, there is a specific research that was conducted to provide recommendations for smart home technologies. Therefore, this report provides some detail on recommendations for Smart Home technology manufacturers and consumers/users in different categories which are web interface, authentication or authorisation, transport encryption, privacy, mobile interface and physical security.

#### 6.1. Objective analysis

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective 1</strong>: Identify and discuss the current smart home technologies available in the market using secondary and primary research methodologies</td>
<td>The section 2 of this project is mainly on the secondary research conducted on the background of Smart Home and the current technologies available in use for Smart Home. The section 4 of this project focus on the primary research conducted to gather information.</td>
</tr>
<tr>
<td><strong>Objective 2</strong>: Collect reliable data on the present availability and security features of smart homes technologies using quantitative and qualitative research methods.</td>
<td>The section 2 of this project is mainly on the secondary research of the security challenges of Smart Home technology usage and the section 4 of this project provide a detailed description of the primary research.</td>
</tr>
<tr>
<td><strong>Objective 3</strong>: Identify the security vulnerabilities of the technologies through my research</td>
<td>The section 4 completely discuss on the facts received from the interview and survey.</td>
</tr>
<tr>
<td><strong>Objective 4</strong>: Provide effective recommendations to address or minimise the explored security vulnerabilities in smart homes.</td>
<td>The section 5, of the report provides the recommendations for manufacturers and users of the Smart Home technologies.</td>
</tr>
</tbody>
</table>

#### 6.2. Future work

The list of proposed additional ways in which the same project can be done is provided below:

- The primary research which are online survey and interview should be conducted over a longer period to cover a larger group of people. The questions used for the interview and survey can remain same.
• The group discussions should be added to the primary research (online survey and interview) in order to get some argument opinions regarding the Smart Home and security challenges.
• Looking into reasons for adoption and if they are in fact security related or there are other drivers.
• View the Smart home security issues more in depth than this project undertook.
• The project should also include the practical security testing of different Smart Home to get observation regarding the vulnerabilities.

6.3. Limitations

There are some limitations identified in this project which are:

• The primary research (interview and survey) was conducted for very limited amount of people, therefore the results received cannot be accurate.
• The time spent on the secondary research is limited as the project overall time is not sufficient to perform a wide range of secondary research.
• The recommendations are provided in general for the smart home technology suppliers and end users. However, the more appropriate way to provide recommendation is to specialise with respect to the technology.
7.0. References


Han, D.M. and Lim, J.H., 2010. Design and implementation of smart home energy management systems based on zigbee. IEEE Transactions on Consumer Electronics, 56(3).


Lutolf, R., 1992, November. Smart home concept and the integration of energy meters into a home based system. In Metering Apparatus and Tariffs for Electricity Supply, 1992., Seventh International Conference on (pp. 277-278). IET.


APPENDIX: Ethics Approval Email

Tarjed's Ethics Number

BH
Berger, Hilary <Hilary@cardiffmet.ac.uk>
Sat 17/12/2016 17:45
Begum Taha 
<thebegum@cardiffmet.ac.uk>, Alaswad, Tahir Akeel M. is

Inbox

Hi Taha, thanks for the Ethics summary form.
Ethics all approved now.
Here is Tarjed's ethics number

20092614 Alaswad Tarjed Comp TB 201606323

Regards
Hilary