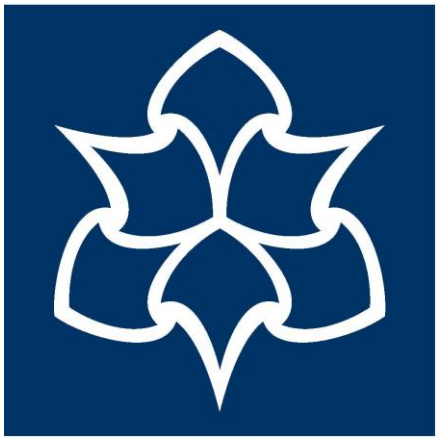
A Smart Home Environment for Users with Physical Disabilities with Practical Security Testing

A DISSERTATION SUBMITTED TO MANCHESTER METROPOLITAN UNIVERSITY FOR THE DEGREE OF MASTER OF SCIENCE

IN THE FACULTY OF SCIENCE AND ENGINEERING



2019

By

[redacted]

Department of Computing and Mathematics

Abstract

The internet of things (IoT) refers to a network of physical objects which are interconnected. The number of IoT devices has risen throughout the years, growing from 15.41 billion devices in 2015 to an estimated 75.4 billion by the year 2025. Commercially, IoT smart home products are being released each year allowing users a smart way to control aspects of their home.

The aim of this work was to firstly, develop an IoT project which would provide an insight into a smart home system aimed at those with physical disabilities. Second, look at security issues which a smart home system may contain. A small factor system was developed mimicking that off a commercial IoT system while still containing all the same functionality. The literature review highlighted serval security issues which can cause vulnerabilities in IoT devices. Research on simple IoT solutions regarding users with disabilities was lacking, with many studies trying to design life changing systems.

The findings concluded that security issues are present within IoT devices and highlighted the changes required to fix these vulnerabilities. The findings also showed how this smart home system can be further developed to create a smart home controlling all aspects of the house aimed at those with disabilities.

Acknowledgement

Thank you to my family for supporting me not just on the hours spent on this project, but on supporting me throughout the course in general.

Thank you to my supervisor Nick Whittaker introducing me into the world of IoT and inspiring me to choose the topic for my project. Your guidance and support were appreciated throughout the process of this project.

Declaration

No part of this dissertation has been submitted in support of an application for any other degree or qualification at this or any other institute of learning. Apart from those parts of the dissertation containing citations to the work of others and apart from the assistance mentioned in the acknowledgements, this dissertation is my own work.

Signed [redacted]

Contents

1 Introduction

1.1 Background

The term Internet of Things (IoT) is used to describe devices that are essentially connected to the internet. However, with the growing trend of IoT the term is used as more of a relation between devices which can "talk" to each other using the internet. These devices usually form a system, which can range from low-powered sensors to smartphones or personal computers. The popularity of IoT has increased over the past few years, in 2018, 7 billion devices were connected to the internet. This figure is set to rise according to the Gartner Report by 20.6 billion by 2020. With such a rapid growth rate, IoT is becoming a forefront to solving some of the worlds biggest problems.

Devices such as the amazon echo, google home, and other personal assistants are becoming used more in everyday life. These devices are now becoming known as "smart homes" due to their capabilities to control and talk to other devices (IoT) within a user's home. Things like, security cameras, lightbulbs, thermostats, kettles, can all be controlled using voice commands with a personal assistant. The main benefit of these IoT devices is that they provide ease of use for users, with a lot of IoT being linked up with mobile applications to control systems from outside of the house.

With the advances of IoT, not only has it made everyday life more convenient for everyday users, but IoT has made life a lot easier for people with disabilities. IoT allows users with disabilities to change aspects of the physical world from within the digital world. A study looked at an overview of the IoT for people with disabilities and believed that IoT can offer people with disabilities the assistance and support they need to achieve a greater quality of life. Research has already been done for people who are physically impaired to see how IoT can improve the quality of their life, all reporting positive outcomes. Body sensors and actuators have been used to detect user's intention to move certain muscles. Smart home systems have been used with mobile applications to allow disabled users to control home appliances. Further research is also being conducted to allow the IoT to help users with disabilities conduct online shopping. With the increasing popularity and developments of IoT, more people with disabilities will be able more independent due to IoT.

Although the advancements of IoT comes with many positives, the negatives of IoT should not be overlooked. The security threat that comes with IoT should be taken serious by all users of IoT devices, whether personal or organisational users. Research conducted earlier this year revealed that many organisations lack the skills to develop, manage and deploy IoT solutions, especially in the areas of data analytics and cyber security. One of the biggest challenges of IoT is to ensure data a privacy is protected. Hackers have already started targeting IoT devices, most recently on baby monitors. With IoT usually consisting of low powered sensors, mobile communication, and near constant access to the internet, hackers are targeting these devices to spread malware throughout the networks.

1.2 Aims

The aims of this project are:

- Firstly, to investigate how components chosen for this project are applicable to create a larger scale IoT smart home system for those with disabilities.
- Secondly, to investigate performance and usability issues closely related to choose with disabilities.
- Finally, to test for any security issues relation to smart home devices.

1.3 Objectives

The objects of this project are:

- Review the following areas: Smart house environments, IoT in relation to disabilities, Security issues within an IoT house environment.
- Analysis and review the laws and ethics, in areas specific to security and users with disabilities.
- Review the range of specific hardware and software for such environments, API's commonly used in IoT projects, databases used.
- Design the smart house environment, show components used in the design.
- Implement the design in developing the system using appropriate API's, cloud servers, and applications.
- Report outlining any security issues with the system, compare the security with other IoT security research.
- Implement the security changes needed to make the system more secure.
- Critically evaluate the system, compare to current research and other IoT devices.

2 Literature Review

2.1 Introduction

This review aims to explore the current trends and research within Smart-Home Environments, specifically in relation to the physically impaired population. This review will also explore the current Cyber-Security issues within Internet of Things (IoT), and review the current problems, solutions, and frameworks that are currently available.

The methodology that was used to research the above topics was to review the following areas: Current Smart Home systems, especially in relation to the disabled population. Current cyber security issues within smart-home environments. Enabling technologies within Smart-Homes and Cyber-Security frameworks.

2.2 Wireless sensor networks (WSNs)

Wireless sensor networks (WSN) are a group of sensors which collect data and forward data to a base station that can monitor and collect this information. The most common usage for such sensors is usually to monitor pressure, temperature, weather etc… WSN are one of the most important technologies that form the basic structure of an IoT system.

2.2.1 Topology

They are many different types of topologies within IoT, such as, Bus, Star, Ring, Mesh, Tree, Hybrid. The basics of network topologies is the ability to provide a certain number of communications between two or more devices (Rouse, 2019).

Many studies (Lim, Kwon and Lee, 2018) have debated which types of topologies work well within the IoT environment to provide the most secure network. A reason to discover the best suited topology is due to various topologies passing data through unnecessary links which increases the chance of data being wiretapped ((Vijayanandh, 2014).

The enabling technologies which perform well within IoT topologies are, Z-Wave, ANT/ANT+, Bluetooth, Near field communication (RFID), and IEEE wireless networks.

2.2.2 Communication

Wireless communication is the process of packets being sent between two or more devices. These packets are usually sent starting at one network endpoint, forwarding the data to a router, that then

connecting other routers which processes these packets on to an endpoint connected to a different network. This is the common principle of how data is sent via networks, however, sometimes sending data throughout the internet can be very insecure. Research into wireless protocols is currently ongoing to developed frameworks or communication standards to make sending data over networks more secure. An overview of some of the most common protocols used in IoT are detailed below.

2.2.2.1 IPv4/IPv6

IPv4 and IPv6 are both internet protocols which is designed to handle advanced network demands. Both protocols are used in IoT, however they both carry their unique benefits in relation. Although IPv4 is slightly faster, IoT IPv6 is a much simpler protocol which requires less processing power for routing nodes (LIN and LEI, 2008). IPv6 seems to be the preferred protocol in IoT due to it being the most up to date protocol providing more IP addresses.

Current research details many articles that are developing their own frameworks using the stated protocols to deal with the threat of security attacks within the IoT field. One study proposed a user network access control framework which allows users to manage the 'things' within a smart home environment. The framework seemed to be successful at making the smart-home more secure. However, the study only used the framework while deploying the IPv4 protocol, and even the study states that IPv6 is the key enabler for IoT (Alshahrani and Traore, 2019). It appears counter-productive to develop a framework using an older and less preferred technology. The main issue is the allocated IP addresses for IPv4 may soon be exhausted, therefore voiding this framework.

The above study is one of many that are looking into the security issues with IPv6, most developing their own security framework using IPv6 aimed at IoT devices (Byun et al., 2012, Shin et al., 2017, Alshahrani and Traore, 2019). Most studies state that IPv6 provides an unimaginable about of IP addresses, great performance enhancements, and increased security which can seem promising at first glance. However, virtually all these studies do not undergo serious security checks within their research.

2.2.2.2 ZigBee

Research indicates that WiFi and ZigBee are the two preferred communication technologies for IoT, especially within smart homes. Zigbee is based on the IEEE 802.15.4 standard (Zigbee Alliance, 2019). Research suggests that ZigBee has certain advantages in comparison to WiFi when it comes to IoT (Thuy Nga, Kim and Kang, 2007). One of the advantages is that ZigBee could provide a low-cost solution regarding energy consumption as oppose to the more energy demanding WiFi (Thuy Nga, Kim and Kang, 2007).

Although numerous studies have looked at ZigBee within IoT, and the comparison of ZigBee and WIFI, little research has been done on the level of security between these two technologies.

2.2.2.3 Z-wave

Z-wave is a wireless communication protocol which is mainly used for home automation. It uses low-energy radio waves to communicate from device to device.

Although the company Z-wave do not inform their customers much about security issues, one study reversed engineered certain aspects of the Z-Wave routing protocol to see what they could discover. The findings outlined that the topology and routes may be modified by an outsider through exploitation. Furthermore, the studied proved this theory by conducting a Black Hole attack to expose these vulnerabilities (Badenhop et al., 2017).

2.2.2.4 Bluetooth

Bluetooth is a wireless technology that sends data between fixed devices, using short-wave lengths. Most Bluetooth devices use either STAR or MESH network Topology (Ensworth and Reynolds, 2017). Bluetooth doesn't seem to be the preferred choice of wireless technology especially within the

area of IoT due to certain issues such as; poor security, low frequency range, trouble to keep signal in poor weather conditions (Wedd, 2019).

2.2.2.4 IEEE 802.15.4

IEEE 802.15.4 is a low power wireless communication protocol which is commonly used in IoT. IEEE 802.15.4 provides high reliability for IoT deployments and is frequently being deployed in IoT home automation systems (Goldberg, 2019). One of the key features of IEEE 802.15.4 is that it supports IPv6 which provides a large array of IP addresses for IoT connected devices. One of the main problems which researchers found (Bhaskar and Mallick, 2015) within IEEE, is that the end-to-end delays in packet transfers could result in data loss, and possible interference can cause increase to power consumption.

2.3 Speech-recognition

Speech-recognition technologies have made great strides within IoT, with many speech-recognition API's being available for commercial and personal use. Some of the major organisations leading the field in speech-recognition technologies are Amazon, Google, IBM.

Research has been conducted to provide speech-controlled cloud-based wheelchairs for users with physical disabilities (Kološvari et al., 2019). One research paper states that for speech-controlled wheelchairs to be commercially available for disabled individuals, future research should look at affordable and accurate solutions to speech-recognition software, especially in terms of error rate (Puviarasi, Ramalingam and Chinnavan, 2014). Kološvari et al. (2019), studied three speech-recognition technologies and found that combining these technologies together using cloud harvesting, you can drastically reduce the error rate. Although this research provided a useful insight into lowering the rate of error, the method wouldn't be realistic due to the requirement of combining competitors.

2.3.1 Google Speech Recognition

Google is one of the major organisations in Speech Recognition technologies. Google cloud speech-to-text API enables developers to convert audio to text by applying powerful neural network models which supports 120 languages (Google Cloud, 2019). Although Google seems to allow an initial trial for the speech-to-text API, they charge a fee afterward this period. Due to this, developing software using Googles API may not be feasible for certain individuals, especially since alternate software is available for free.

Google Home is a smart speaker that allows connectivity and control of devices through Google Assistant within IoT. Although the popularity is increasingly for the Google Speech Recognition software within the area of IoT, a study was conducted detailing the error rate of the Google Web Speech API. The study found that only a minority of all spoken sentences are recognized correctly (Anggraini et al., 2018), which emphasises the point discussed earlier, that Speech-Recognition technologies maybe lacking accuracy in terms of error rate.

2.3.2 Amazon's Alexa

Alexa is Amazon's cloud-based voice recognition software that allows plenty of customization which gains advantages on competitors. Commercially, Amazon Echo is a smart speaker that uses the Alexa technology to perform different functions via voice control.

The main advantage when comparing Alexa to other voice-recognition software is the ability for developers to create custom Alexa Skills. AWS Lambda is a service that lets you run code in the cloud without managing servers (Amazon Web Services, Inc., 2019). Developers can write Lambda functions in a variety of different programming languages, increasing Amazon's overall target audience. Alexa also contains a smart-home API to help develop software within the area of IoT.

2.3.3 IMB Watson Voice Recognition

IMB Watson speech-to-text software transcribes 7 languages in real-time. IBM claims that the software is highly accurate (Ibm.com, 2019), however previously discuss research states that the main problem with speech recognition technologies is error rate, questioning the viability of the term "highly accurate".

IBM Watson also comes with custom API, SDKs, and the required documentation for developers to use. IBM's cognitive technologies are currently embedding Watson software into soundbars and alarm clocks which users can interact with using natural language (Ibm.com, 2019).

2.4 Home Automation Systems

Home Automation systems are becoming increasingly popular for average users. More people are upgrading to smart home systems for their house due to the increasing trend, reduces in costs, and more advanced technologies providing more control.

Although useful for anyone willing to invest in IoT smart home systems, these IoT devices can be especially useful for those with disabilities. The main issue faced is that commercial smart home devices like the ones detailed below, all control a certain aspect of the house and not the entire building.

Currently several smart home systems are commercially available. These include, Philips hue for light control, Ecobee4 for Thermostat control, NetGear Arlo Q for security. However, not one of these devices can control every aspect on the house. Software is available like the Wink Hub 2, and Samsung hub to control multiple devices, however question on how reliable these devices are for users with disabilities needs to be reviewed.

2.5 IoT for people with disabilities

IoT devices are constantly improving and bringing more solutions to everyday problems, especially regarding helping people with disabilities. An interesting area of IoT is the development of IoT devices/systems to increase the life quality of individuals with disabilities. Cyber-physical wheelchairs, self-management systems, RFID tags for disabilities, smart-cities and smart-homes are some examples of research already been conducted for this area (Rashid et al., 2017).

2.5.1 Physical Impairment

IoT can help peoples with physical impairments overall life satisfaction by giving these peoples more independence. Although some research within this area has been conducted, the overall research within the area is still in the early stages.

Research into the cloud-based speech-recognition software is currently on-going to provide an affordable and accurate solution to develop speech-controlled wheelchairs (Škraba et al., 2015). Currently MIT intelligent wheelchair project uses sensors to perceive the wheelchairs surroundings, a speech interface for commands, and a wireless device for room-level determination (Rvsn.csail.mit.edu, 2019). Although this would be an astonishing leap in technology, certain things like power-efficiency, size of systems and portability are becoming the main challenges.

Another interesting area of research are components designed for the physically impaired such as: body sensors, actuators and neurochips, RFID technology with body sensors (Domingo, 2012). This research opens a different angle when looking at IoT devices aimed at the physically impaired. This field is a long way off being commercially available due to many challenges, research suggests that improvements within wireless networking one area needing improvement (Pirbhulal et al., 2016).

2.5.2 RFID

Radio Frequency Identification (RFID) technology is a well-known wireless application for traceability, logistics, and access control (Bonsor and Gadgets, 2019). RFID is now a standardized technology and is used almost everywhere due it to its inherent advantages.

RFID could be a gateway to helping those with physical impairments. Some cities around the world have already started using RFID tags for people with disabilities to control traffic signals by indicating they're at road crossings (Rho, 2014). One study suggested the development of smart cities to use RFID tags to check prices of items on high shelves that people cannot reach while they're shopping (Rashid et al., 2017).

2.5.3 Smart homes

The increasing popularity of smart homes are bringing more ease of use and customizability to the everyday consumer. Smart home technologies assist with control, enhancement, and automation within the home environment. A typical smart home environment will consist of sensors, smartphone applications, Wi-Fi hubs, commonly designed to work with home appliance (Abowd, Edwards and Grinter, 2003).

Smart homes are useful when it comes to helping those with disabilities. The ability to control appliance from a smart phone can bring a new level of independence. One study suggests that monitoring people with disabilities remotely can reduce the presence of caregiver all day long and having smart homes will allow persons with disabilities to check on everything without moving, therefore increasing independence (Storey, 2010). However, creating a smart-home environment where most appliances are considered smart can be costly, and elderly peoples with disabilities may need training to use certain technologies.

Many studies (Istomina, 2019, Hsio-Ting, 2017, Chen, 2017) are researching IoT devices which aim to aid in everyday life for peoples with disabilities. Car internet cyberbiological system, image recognition for delivered meals, also Morse-code smart home control are all currently being proposed. However, many devices seem unnecessary complicated and overengineered.

2.6 Security

When it comes to IoT for people with disabilities, they can be certain challenges which are faced, especially within privacy and security. In 2014, it was revealed that there was a large-scale attack on IoT devices including TVs and fridges, with hackers believed to have broken into more than 100,000 everyday consumer gadgets (Sivaraman et al., 2018). This is extremely worrying, especially when those with disabilities are considered being more vulnerable (Ali and Awad, 2018).

A study analysing the most popular available smart-home devices such as the Phillip hue, baby monitors, security devices to find that all had some form of vulnerabilities (Lin and Bergmann, 2016). Many of these companies assure that their devices have appropriate security, however, this article proved it not to be the case.

2.6.1 Blockchain

Blockchain technology was designed for the Bitcoin tech community, however in recent years it's found potential uses for other technologies. A blockchain is a network of nodes which processes and verifies transactions. Each group of transactions is known as a block, which cannot be changed (Rosic, 2019). Many believe (Khan and Salah, 2018, Miloslavskaya and Tolstoy, 2018) that blockchain technology is the future when securing IoT devices, with one study (Malviya, 2016) believing that blockchain can be a key enabling technology for providing viable security solutions to today's challenges in IoT problems.

Although Blockchain is an excited technology for the future, research on IoT security and blockchain is limited, with most of the work being focussed on leveraging blockchain technology to benefit IoT in general. The drawbacks on using blockchain is the increase of resources, which would require more energy to use the protocols and algorithms. Like all technologies when considering security in IoT, blockchain can also be vulnerable and effective mechanisms need to be further researched before the technology can be deployed.

2.6.2 Network-Level Approach

When reviewing the broader scope of internet security in general, they are four main levels of security; system level security, network level security, application level security, and transmission level security. Most computers whether for business or personal use have the processing power to enable a good standard of system level security. However, some nodes within IoT do not have the processing power for system level security, therefore research has been done on the network-level to secure IoT devices (Sivaraman et al., 2018).

Security management provider (SMP) develops, customizes and delivers to the user extra safeguards at the network level for the IoT devices in their household (Borgia, 2014). The SMP is used to authenticate devices so attackers cannot take control over devices. This could add another level of security to IoT devices, with research suggesting that nearly all commercially available IoT systems are easily hackable. Although the above research boasts promising solutions to increase security, the study was conducted in 2015 and since then no further research or developments have been developed.

Another research paper suggests using the IPSec protocol that secures data exchange at the network level (CAI, 2008). However, they state it cannot be directly applied to the IoT environment for several reasons.

2.6.3 Algorithm Approach

Within the technology sector another rapid area of growth is machine learning and AI. With more advancements in algorithms and better computational power to process large amounts of data, these techniques can be useful within IoT.

Research has already been done on an energy efficient security algorithm namely Triangle Based Security Algorithm (TBSA) which is used for data encryption. With respect to real world IoT applications, security threats are becoming a major issue, especially in relation to data transmission. Another study (Alotaibi and Elleithy, 2016) used random forests to detect whether Mac addresses were being spoofed, with surprising accuracy.

The above research provides another element of security which can be utilized within IoT devices. Although promising, IoT security algorithms are still in their infancy and further research needs to be conducted before they can be used within IoT systems. Protocols and algorithms are the costliest in terms of energy consuming which is already a major issue within IoT.

2.6.4 Vulnerabilities

Research on how to deal with IoT vulnerabilities is still on-going, with the regular releases of new technologies also comes with an increase in security vulnerabilities. It has already been stated that most commercially available IoT devices have some sort of vulnerability, with one study stating that any vulnerabilities exploited after deployment becomes difficult to detect and alleviate (Khan and Salah, 2018). It’s therefore important that a solution to fixing vulnerabilities on deployed systems is studied.

(Shin et al., 2017) proposes that a standard protocol is needed across all IoT devices to detect and alleviate infected device. He further explains that a verification protocol is essential requisite for

harnessing the IoT security. Most studies within IoT detail that additional verification seems to be a promising solution when securing devices.

2.6.5 Types of Attacks

Securing IoT devices from attacks remains a formidable challenge. The large array of IoT devices makes security vulnerabilities diverse and attack vectors manifold (Madhugundu, Ahmed and Roy, 2018). It's therefore essential when securing IoT devices that knowledge of at least the most popular attacks is known.

2.6.5.1 De-authentication Attack

A de-authentication attack is very common not only within IoT, but within network security in general. A de-authentication attack allows attackers to use just a few simple commands to remove clients from a network. Once the jamming of the network has stopped and clients reconnect, attackers can capture data, most commonly known as a handshake to crack passwords.

Westerlund, (2019) showed how a user remotely piloting a drone could de-authentication from the device and a hacker take control. If an attacker is ready with another controller then the drone can immediately be connected and flown away. Companies like amazon are testing drones to deliver packages, but a simple attack can be dangerous and costly for a company.

It is expected that most cars will be "smart" cars in the future, with companies like tesla already producing self-drive cars. The software and architecture drones and self-drive cards do not differ too much, which displays how dangerous such a simple attack could be. In relation to users with disabilities, more specifically smart wheelchairs, it's important that these types of attack situations are addressed.

2.6.5.2 Spoofing

Spoofing can be described as falsifying identity and taking the identity of another system. If a system is sending information to a certain IP address, a spoof attack would take the form of this IP and intercept the data. ID spoofing within IoT is a main cause of concern and can cause problems within a network, spreading malware or using machines for malicious purposes.

Mansfield-Devine (2011) states that internet protocol security techniques are not effective for adoption in the IoT infrastructure against ID spoofing and reply attacks. There purposed framework, PRIG, ensures a cryptographically secure yet lightweight ID generation for the devices. However, this framework would be hard to adapt for all IoT devices and additional measures must be created in order to do so. Another study (Reddy and Nirmala, 2016) has proposed a low-cost GPS spoofing detector for IoT devices by detecting anomalies. Although the study is promising, it only seems to target GPS spoofing.

2.6.5.3 Intel gathering

Intel gathering is a less serious attack in-term of potential damage inflicted, however it's still a serious threat within IoT. With denial of services it's possible to spy on networks and gather intel without being connected to a given network. A hacker could see which devices are connected to a given internet and allow for denial of services' attacks to be conducted. The main issue within IoT is smart-home systems using devices like Amazon Echo is they are likely to have a constant connection to the network, therefore making intel gathering constantly available.

2.6.5.4 Man-in-the-middle

Man-in-the-middle (MitM) attacks are a popular method for gathering data being sent via the internet. The main issue with main in the middle attacks is that a large amount of IoT devices have OpenFlow channels. A MitM would utilise these methods by intercepting data and sending possible malicious data back to the source.

One study shows an example of the MitM attack and a proposed countermeasure to stop the attacks. They use a bloom filter to detect any packets that have been modified in anyway (Li et al., 2017). Other studies have also developed countermeasures for the MitM attacks; however, they use the checking methods rather than detect misbehaving switches.

2.6.5.5 DDOS

Distributed denial of service (DDOS) attacks are one of the most common attacks within internet security due to their simplicity. The main principle behind DDOS attacks are to flood the bandwidth of target systems. Botnets go hand-in-hand with DDOS attacks, they have been used to launch DDoS attacks affecting the internet infrastructure (Ceron et al., 2019). The issue with Botnets is the ability to control IoT devices for DDoS purpose. With the growing amount of IoT devices currently connected to the internet, this could have devastating effects. The Mirai malware peaked in 2016 at 1.1 Tbps of network traffic, attacking French webhost and cloud services. With cloud service being the main data source for IoT devices, it's a critical issue if any of these cloud servers become compromised.

2.6.5.6 SQL Injection Attack

One of the problems with IoT devices that are controlled by certain smartphone applications is the possibility of being vulnerable to SQL injection attacks. With a simple command an IoT device could be compromised, this is especially important within IoT hobbyists and enthusiasts who may use their own databases for IoT projects. Previously talked about botnets are also said to be able to perform SQL injection attacks (Kh, 2017).

Anonymous developers of an IoT worm known as Hajime claims to be fighting this epidemic (Moos, 2017). The self-proclaimed worm has assumed access to over 300,000 IoT devices and updated security patches to thwart SQL injection attacks.

2.7 Communication protocols

2.7.1 JSON

JavaScript Object Notation (JSON) is a lightweight language used to exchanged data. It's relatively easy to use with great performance. JSON has become very popular to represent data in the upper layers of the IoT domain (Hao, Wang and Shen, 2018).

Software like AWS uses the JSON protocol to send data to and from devices. Many of the smart-home devices available on the market like Phillips Hue or Evohome mainly use HTTP protocols to send data to the cloud. However, most developer API's that link with these devices use JSON.

JSON doesn't come without its downsides though, especially where privacy is concerned. With one study stating that JSON can carry malicious data that could be hard to detect due to the encryption (Yoo, 2014).

However, another study states that JSON is a better alternative to the widely popular XML. XML is also a language used to transfer data, however, JSON is becoming the preferred method, especially where IoT is concerned (M.Kom, 2016).

2.7.2 HTTP

Hypertext Transfer Protocol (HTTP) protocol is a data transfer technology that uses two main methods, GET and POST. Get is used to retrieve data from a URL, whether that's a database store in SQL or retrieving data from the JSON format. POST is the opposite of GET, instead of retrieving data from a URL it sends data.

Many IoT systems such as Philips Hue, Evohome, Amazon Echo use HTTP requests to call data from the cloud servers and send it back to the local router. HTTP is one of the more preferred data protocols throughout the networking's lifetime.

The main issue with HTTP is potential with encryption. HTTP send data in plain text, which if compromised by a hacker can view all data without having to break any encryptions (Buchanan, Helme and Woodward, 2018). This can be extremely worrying in organisations where sensitive data could be sent between devices.

One resolve for this issue is using Secure Hypertext Transfer Protocol (SHTTP) and Hypertext Transfer Protocol Secure (HTTPS) which uses client-side encryption. However, research shows that SHTTP and HTTPS still have security issues (Musliyana et al., 2018).

2.7.3 MQTT

MQTT (Message Querying Telemetry Transport) protocol is a publish-subscribe-based messaging protocol. MQTT is optimized for high-latency or unreliable networks and is mainly used for small sensors and mobile devices. Due to this, it's an excellent protocol to use for IoT.

MQTT works on top of the TCP/IP protocol, which is mainly used for machine to machine data sending. MQTT has become adopted as a common protocol with IoT systems, however, it doesn't come without its drawbacks. IoT systems with many nodes sending a constant stream of data can result in traffic congestion (Park, Kim and Kim, 2018). This could also result in data loss and inaccurate overall data from the sensors. It's also been reported that due to the large amount of traffic that could be sent via MQTT, the protocol is prime for a DDOS attack (A. P. and K., 2019).

3 Problem Analysis

3.1 Literature Review Conclusion

This would stop add another security element to RFID cloning, and social engineering attacks, as well as adding more usability. A basic security test needs to be overviewed to outline the risk that peoples with disabilities could face within IoT systems.

3.1.1 Usability

It's important when developing products for users that have physical disabilities that software and hardware are both easy to use and simplistic. It's imperative that an android app is created alongside voice control to tackle the challenge of physical impartment. Research outlines that peoples with disabilities are increasingly vulnerable especially when it comes to privacy. RFID tags and smart cities are already improving life satisfaction by providing ease of use in cities. Research has also been done on smart wheelchairs, although this research is a long way off commercial use.

When considering security and privacy aspects of smart homes with individuals that have physical impairments, it's crucial to implement a foundation of both physical and cyber security. Therefore, it's important that the system design has a camera from which the user can view images via a snapshot of visitors waiting to enter the house. For this design to be successful it's important that the software is simplistic and well presented.

Other usability aspects of the project must also fit into the criteria suitable for users with physical disabilities by following research reviewed in the previous chapter. Any software and hardware will have been built based on usability.

3.1.2 Security

The research regarding security, cyber-attacks, and IoT vulnerabilities provides ab insight into important issues faced within IoT. Researchers have conducted experiments which could be flawed or

also contain security issues in some form of way. It's been outlined in many articles that a standardized protocol and framework for IoT security needs to be further developed.

One study considers the five most important security goals for smarts homes: Authentication, Authorization; Confidentiality; Integration; Availability (Alshahrani and Traore, 2019). Many articles have boasted new advancements that are believed to solve the IoT security crisis, however some articles were published 4+ years ago and the proposed frameworks have never been mentioned since publication. One common trend however is the research into one of the five security areas detailed above.

A common research trend within security seems to be another form of authentication for IoT devices. Research suggests this would solve many of the IoT attacks that are currently happening today, and authentication is a relatively low-cost and easy to implement solution. Although in principle this technique could be very affective, a question needs to be asked whether users would feel it's necessary for additional authentication. Many users of the internet do not take security threats too seriously and may find double authentication a tedious task. Currently, remotely controlling a smart-home system would take a couple of seconds. The added element of additional stages of authentication could be more effort for users than its worth.

It's therefore important that a focus on this project is looking at authentication. One aspect that needs to be considered is the usability of additional authentication within people with disabilities. If extra steps must be taken which increases the overall time it takes to open a door, it could defeat the purpose of the system.

The main trend in topic seems to resolve around the power consumption and processing power that many IoT devices face. Nodes can be targeted as an entry point for hackers to gain access onto the network, and most nodes don't have enough processing power to handle security protocols on the device. Different approaches to this problem have been purposed, from network-level security protocols to authentication techniques. However, many believe that it's simply a case of waiting for technology advancements to provide more process-power.

3.1.3 Programming Languages

The programming languages chosen within this project were selected based on the requirements for the project. A smart home design which allows the system to be controlled externally requires multiple languages and software working towards the same goal.

- Java is an object-oriented programming language (OOP) which comes pre-installed on almost every device world-wide. It's the main programming language which is used with android studio to develop an application for the project. Java features many usable libraries which can aid developer of IoT devices, which will be discuss in later sections.
- C/C++ is the main language which is used for the Arduino IDE used in this project. Once it was identified that Arduino IDE would be used within this project, the programming language was automatically chosen.
- PHP is a popular scripting language which is suited to websites, web applications, and backend design. It's a useful language to bridge programs with databases to retrieve and send data via certain protocols. PHP will be used in many instances on this project, also featuring HTML and CSS.
- JavaScript is one of the core technologies used in websites throughout the world. Although PHP and JavaScript almost compete for the same tasks, both will be utilized within this project.

3.1.3 Communication Protocols

This project features a mobile application, a website, and a smart-home system. They are numerous gateways within this project for data to be sent from one endpoint to another. For this reason, different protocols are used within this project:

- MQTT was chosen as the main communication protocol for this project. MQTT offers the subscribe/publish features which is extremely useful when considering an application, website, and amazon echo all have the same end-goal. MQTT allows a light-weight choice to track the opening and closing off the door from different endpoints. The PAHO-MQTT library is especially useful within this project as it allows a cloud-server to be used for the project which can be easily implemented within different programming languages.
- The HTTP protocol is also used within this project. The language is chosen for a specific task, uploading an imagine to a website. For this simple feature, it's important that a protocol was chosen that is both lightweight and easy to implement.

An issue was reported within the literature review detailing the possibility of congesting in relation to sending data via MQTT. When considering the smart home system that will be designed in this project, data sent via MQTT will be very minimal when compared to organisational IoT devices. Therefore, the issues faced with MQTT will generally not impacted a small-scale system as much, if at all. Companies such as Facebook also use MQTT for their messaging services and are managing MQTT attacks.

3.1.4 Integrated Development Environment

It was important that each technology chosen for the project would suit a specific task that needed to be accomplished. For this reason, the IDE chosen needed to:

- Support the hardware being used for the project
- Consider the software needs/goals
- Work with a range of different libraries
- Support features that help with usability

For these reasons two IDE's were used for this project, the Arduino's IDE and android studio. The Arduino IDE offers plenty of support and usability for IoT devices which are connected. It features libraries which can be directly used on the ESP WIFI modules.

Android studios is also used for more obvious reasons, to allow easy deployment to android applications. Android studio also provides improvements for future work, to allow control of IoT devices on android applications and tablets. The main positive of choosing android as oppose to an iPhone application is the ability to install android on almost any device and run the application. This is especially useful for future work involving a general control panel.

PHP, JavaScript, HTML, and CSS have all be written using Notepad++. This project is to show the functionality behind a website and an application. Therefore, it was not necessary that a more powerful software such as Adobe Dreamweaver be used for the writing and design of a website.

3.1.5 Hardware

When it comes to hardware which can be used in smart-home systems, products can be plentiful. Many hardware alternatives are available on the internet which can be used with alternate software to produce similar results. This project is not a review of certain IoT hardware currently available; however, justification of why certain hardware was chosen will be noted. The below topics will

discuss hardware chosen for this project and a brief overview of similar products which could also be used.

Cost, time-management, scale of the project were all factors in deciding which hardware to use for the system.

3.1.5.1 Arduino

Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are useful for a variety of different reasons and are a popular choice among hobbyists and enthusiasts. Arduino comes with both hardware (Arduino boards) and software (IDE) which are both easy-to-use and adaptable to any environment.

When it comes to smart-home automation many technologies are available like the Arduino board. The raspberry-pi can perform a similar task to the Arduino but isn't chosen for this project due to a variety of reasons. The raspberry-pi comes packaged with prebuilt WIFI enable which would remove the aspect for the ESP8266. However, this solution doesn't come without any drawbacks. The raspberry-pi is an extremely powerful device compared with the Arduino board, therefore naturally making it more power consuming. This system would not benefit from using the extra processing power that the raspberry pi contains.

3.1.5.2 Amazon Echo

IBM currently have a $200 million Watson IoT global headquarters in Munich. Google are developing new products related to there google dot. However, when selecting voice recognition software for this project, Amazon's Alexa seems to be the best solution. Amazon's API's and AWS services are simplistic for developers to create their own skills which also link up to custom mobile applications and smart-home devices. Research has been progressing on linking multiple voice recognition software together to eliminate less margin for error. However, the solution to lower error rate by linking multiple systems is still in its infancy.

Amazon Echo is a smart speaker product released by Amazon that uses voice recognition, intelligent assistant capabilities with a speaker to provide additional functionality. The advantages of the Alexa voice recognition software have been previously discussed within this paper. Amazon's public API's allow Alexa to be ran on devices such as the raspberry Pi and/or used with a custom speaker. However, these are unnecessary steps to be taken for this project.

Alexa's are designed to use wake words (Alexa by default) to activate listening and send data based on commands. However, many are concerned that Alexa is constantly listening and sending data to the cloud. Although Amazon deny this is the case, many researchers are providing ways to detect and remove data being sent (Chung, Park and Lee, 2017).

Alexa sends data via to Amazon Web Services (AWS) to query the cloud data and returns the relevant action. The data sent uses the HTTP protocol containing a JSON body (Developer.amazon.com, 2019). The AWS provide an opportunity for developers to create their own custom skills which can be queried by the Alexa software.

The review above states how the Amazon Echo is a popular choice of smart speakers, in comparison to Google and other products. The open source develop has produced certain libraries like the Fauxmoesp to help with the development of smart home systems. When considering peoples with disabilities perform becomes a main factor when choosing a smart speaker, although research shows that all available voice recognition devices have similar error rates. Similar projects have also been used with the Alexa software have been to help individuals living with dementia (Firth et al., 2018).

Amazon Echo is used within this project to offer voice control for people with disabilities. It's possible that it could take an increasingly amount of time for a person with disabilities to check an

android application or website than the average person. Therefore, while someone is waiting at the door it's important for peoples with disabilities to quickly allow or deny entry into the property.

3.1.5.3 ESP8266

The ESP8266 is a low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capabilities. ESP8266 is a popular choice among IoT systems due to the cost and low power-consumption.

The ESP8266 can act as an access point for devices such as the Amazon Echo, allowing the echo to communicate with the device. The ESP8266 uses HTTP protocols to communicate and send data across a network.

Many IoT systems have been released using the ESP8266 has the communication device, especially smart-home devices (Zakariyya, 2017, Hutabarat, Budijono and Saleh, 2018). The device has also been used on IoT systems to monitor infant incubators and detect heart attacks (Sihombing et al., 2019, Firmansyah et al., 2019).

Due to the low-powered, high capabilities of the ESP8266 it is chosen for this project.

3.1.5.4 ESP32-CAM

The ESP32 is built from the same model as the ESP8266 and provides similar functionality. It contains onboard memory which can store images captured from a local IP address. This feature can be especially useful when saving many images to test for facial recognition.

Although cameras were once bulky and large by size, today the ESP32-CAM sits at around 3cm by 2cm. The literature review outlined how small factor cameras are becoming a growing issue for privacy concerns within today's society, especially cameras which can be embedded into devices such as glasses.

Although this project will not be capturing any pictures of externally individuals, it's worth noting that a camera placed above a door could be a growing concern for privacy. It's therefore important to mention that if such product was to be commercially released, correct management of images would have to be implemented to delete photos from the database.

One major limitation of the ESP32-CAM is only one user can only connect to the server once at the time. This means if the ESP32-CAM wanted to performance two different tasks it wouldn't be possible.

3.1.5.4 RFID

Radio-frequency identification (RFID) refers to technology whereby digital data encoded in RFID tags are captured by a reader via radio waves (process et al., 2019). RFID is one of the major technologies within IoT and is useful within smart-home automation.

Previously reviewed research outlined how RFID tags could help peoples with disabilities in cities. The similar techniques could be used to remotely open a door that otherwise would be impossible to push open.

RFID will add another element within this project, provided security and privacy for users with disabilities. Although the literature review details how RFID cards are known to 'cloning', a method which takes the card and copies for the data for falsify entry. In this project RFID cards will be used for residents to let themselves into the property.

3.1.6 Operating System

Usually projects would not require mention of specific operating systems, although it's worth a mention for developing this project. Each operating system allows different applications to run natively. While testing security issues for this project, companies like HAK5 develop software which

runs on both windows and mac to test for security issues. However, for this project open-source software which runs natively on Linux will be used.

The Kali Linux distro was developed with cyber-security and penetration testing in mind. Security software comes pre-installed onto the operating system and is usually ready to use to test security of devices. Although other systems such as parrot are becoming increasingly popular for security testing, the simplistic features of Kali Linux are enough for this project.

3.1.7 Software Development Methodology

Within the technology industry many use certain software development methodologies to aid with development of projects. Historical evidence points towards the waterfall methodology become the most popular choice. However, recently many companies are adopting the agile methodology for their preferred way of working (Vijayasarathy and Butler, 2016).

Although this project will not review or evaluate how certain methodologies can help a project be developed, it's worth noting that this project will use the agile approach, more specifically using Scrum. Scrum is an offset of the agile methodology and is believed to be an efficient approach to development.

3.2 Conclusion

It was calculated that around 8.4 billion IoT devices were in use in 2017, it is estimated that this figure will rise to 20.4 billion by 2020 ((Knoll, 2019). An overwhelming interesting in IoT has been shown by the industry, academia, and hobbyists alike. It's been declared that IoT could be the next disrupting technology since the internet (Madakam, 2015).

Research has shown us that security issues within IoT is increasing at an alarming rate along with the rapid growth of IoT. Standards, frameworks, protocols, have all been proposed to help organisation secure more IoT devices. Although issues aren't necessarily being resolved, research in the field is still plentiful and progressing.

The findings from the literature review detail promising advancements for users of IoT devices that have physical disabilities. Smart wheelchairs are an interesting topic of research due to the independence it would provide to a user. Although many researchers are looking at elaborate ways to implement IoT devices for the users with disabilities, research lacks on simple systems which can make a major impact for individuals with disabilities. Many reviews have been done on disabilities and current smart home systems available today. However, not one specific smart home device is tailored towards people with physical disabilities or disabilities in general.

Due to the nature of people with disabilities, security and privacy must be taking very seriously with research showing what attacks could do to smart-cars and drones. It's important that usability is a central focus to allow individuals to gain more control over their privacy.

More research needs to be conducted on the types of attacks that could be especially dangerous towards individuals with disabilities. Unlike organisational threats, those with disabilities become increasingly vulnerable in their own home once they start adopting IoT systems such as smart homes.

Although it can be argued that many smart-home devices can offer great benefits for peoples with disability, no leading commercial product specialises in this field. It's essential that extra consideration on usability, ease of use, and extra security/privacy must be implemented to make smart homes more disability friendly.

This project therefore proposes a design for a smart home system specifically designed for individuals with physical disabilities.

The aims of this project are:

- Firstly, to investigate how components chosen for this project are applicable to create a larger scale IoT smart home system for those with disabilities.
- Secondly, to investigate performance and usability issues closely related to choose with disabilities.
- Finally, to test for any security issues relation to smart home devices.

This project is not trying to develop a new system which can only be used by those with disabilities. The purpose of the project is to investigate the components that make up a system so they can be developed into a utopia smart home system aimed at those with disabilities, instead of just a smart home system controlling one aspect.

3.3 Scope

When overviewing this project there were certain aspects that had to be considered before any product or research could be undertaken. Firstly, the timescale of the project had to be taken into consideration with only around four months to complete the entire project. Secondly, the cost aspect of the project would have to be taken into consideration. Testing multiple devices in multiple environments was just not feasible. Lastly, ethics and privacy were all taken into consideration when developing this project.

With the timescale influencing the project, a small scale smart-home system will be designed. However, the proposed design will have all the same functionality as a full-scale commercial smart-home product. Due to privacy and data protection laws, alongside university ethics rules, the project will be tested by the researcher and no external individuals will take part in the project. Although no users with disabilities will be testing the product, the project still provides a useful insight into IoT smart home devices tailored for users with disabilities.

The project will consist of an array of different software/hardware all working in one smart-home model. More detail of each individual technology will be further discussed in later sections. Smart-home systems have advanced rapidly over the years with new technologies constantly being commercially available on the market. However, this project will not try to invent any new technologies or make advancements in this domain.

This project will provide an insight into IoT security issues in a smart-home system. The project will solely focus on issues related to smart-home environments and review attacks that could cause individuals with disabilities problems.

The project will be tested with usability in mind and will be designed using the agile scrum methodology. The scrum methodology allows the researcher to test the design for security issues and implement the changes required.

This project will produce two outcomes, firstly, an insight into a smart-home system focussed on users with physical impairments. Secondly, an overview of simple security issues that users with disabilities could face within such environments.

3.4 Ethics

The ethics for this project will align and follow university ethics regulations.

Due to the aims aligned with this project, no additional participants will be required. Therefore testing of images will require no participants and the still images will hold no human data. However, privacy is still worth mentioning as cameras capturing imagines and uploading the data is a growing area of concern (Serpanos and Papalambrou, 2008).

4 Design

This project will develop an IoT smart home system which will take into consideration the needs of those with physical disabilities. The software, hardware, and methodologies chosen for this project will reflect on current research and the aims of the project.

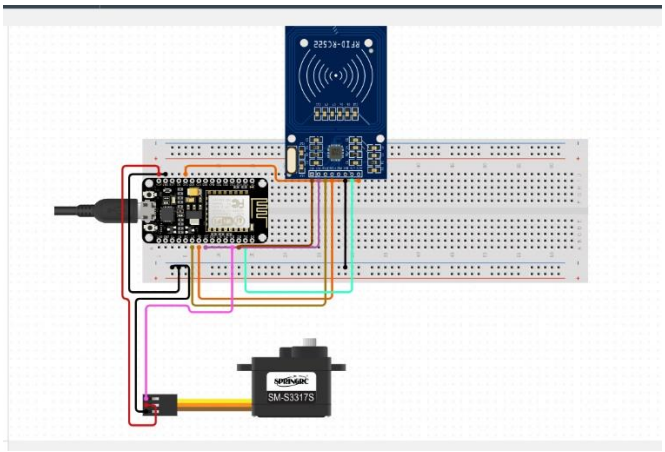
This project will be a small-scale system mirroring that of a fully developed commercially smart home systems previously reviewed. Details on why the project chose a small-scale system were discussed in previous chapters.

4.1 Hardware Design

The physical design will consist of two sets of circuits, one which handles the control of the door, the second controlling the doorbell and camera software. Both these circuits operating together make up the fundamental design of a smart home system tailored towards users with disabilities. The servo used in this project will mimic that of a door hinge.

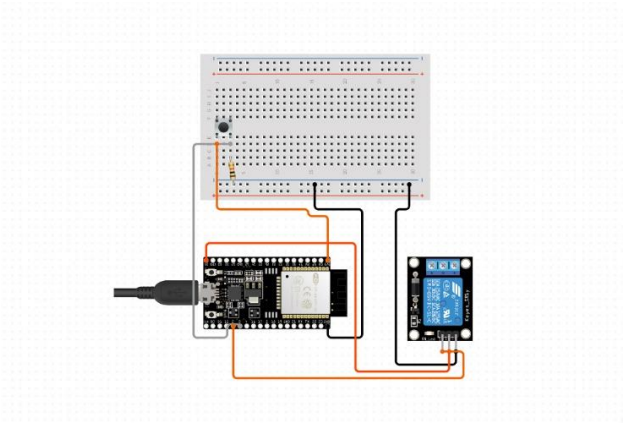
The first system will allow control of servo via three endpoints, Amazon Echo, Android Application, and Website Interface. It's therefore important that an adequate communication protocol and wireless device is used. Section 2.2.2.1 in the literature review, states the benefits of using IPv6 communication protocol. This protocol will be used with the ESP8266. Furthermore, due to reasonable performance, low-costs and low power-consumption the ESP8266 has being chosen. Devices like the raspberry-pi come with a built-in wireless interface, although this would be unnecessary hardware and processing power for this project.

MQTT will be used for the communication protocol with the Amazon Echo, Android Application, and Website subscripting to the topic of door control via MQTT cloud. The ESP8266 will be the bridge between the servo controller and the power supply, handling whether the door will be opened based on the MQTT broker. The below diagram shows the circuit connections between different nodes.



The diagram shows that an RFID will be connected to the circuit for RFID cards to open/close the door. The benefit of using the MQTT with the ESP8266 is to easily control the state of the system regardless of which end-point controls it.

The second circuit will control the doorbell and the camera via ESP32-CAM. One of the benefits of using the ESP32-CAM is the ability to control different components via pins. Other similar hardware such as the mentioned raspberry Pi camera would require the Rapsberry-Pi to function, overcomplicating the system.



The diagram above shows the circuit and wiring of the ESP32 system. The pushbutton mimics that of a typical doorbell, once pressed activates a relay providing power to the ESP32. Using a relay will provide power to the ESP32-CAM for a set amount of time. This time will be evaluated depending on how long the ESP32-CAM takes to send an image to the website via the HTTP protocol. The HTTP protocol is one of the simplest protocols and great for single POST requests. One of the limitations states in the review of the ESP32-CAM was the ability to only view the server once at a time. Therefore, the method of capture a video on the onboard storage and uploading via HTTP will be implemented.

The diagrams of the two systems will be a very close representation of what the final product will look like. However, simpler solutions to make the system smaller will be analysed and the breadboard is likely to be shared.

4.2 Software Design

4.2.1 Programming Languages

Referring to the review in previous sections the main programming languages selected for this project are:

- Java
- C
- HTML/CCS/JavaScript
- PHP/SQL

C/C++ is the main language used for development of Arduino devices. Therefore, the source code implemented on these devices will be written in this language. Java will be the language for developing the mobile application. All remaining languages will be used on the web design aspect of the project.

4.2.2 Software Libraries

When designing the project, it's important to review the current resources available to help with the building of software. Many programming languages feature libraries and API's which assist with building and implementing software.

MQTT Paho is an implementation of MQTT which is available on various platforms and programming language. This project uses MQTT Paho in Arduino IDE and Android studios to send MQTT data to the cloud. Paho allows simple setup of the cloudMQTT server to give applications the correct framework to write/subscribe.

As mentioned in the literature review, voice control will play a huge part in making smart home systems more friendly for users with disabilities. Many ways of implementing voice control with IoT

projects using Alexa are currently available, such as NodeRed, Alexa Skills etc… However, Fauxmoesp is a library which works with the ESP8266 to allow easy control from the Amazon Echo. The main functionality of the library is to emulate a Belkin Wemo device, allowing control over a device. This takes away the need to create a custom Alexa skill which will use more resources and provide the same outcome.

ESP8266 and ESP32 libraries are used to provide functionality to the physical boards. It allows the Arduino IDE to handle input devices and uses of the onboard interface. These libraries are required for the Fauxmosep library to be used.

4.2.3 Usability

Users with physical disabilities could possibly take longer to perform physical tasks such as opening and navigating required software. The positive solution to this issue would be voice control via Amazon Echo. However, control from outside the home would require use of either an online interface or mobile application. It's important that the design of the website and mobile application take into consider the needs of a user with physical disabities.

One of the aims of this project is to test how smart home systems can be used specifically for users with physical disabilities. Therefore, it's not essential that the website and the mobile application are up to designer standards. Although, basic usability and functionality will be required to support the projects aims.

Android studios will be used to develop the mobile application. Android Studios is an excellent software package due to the extensive UI tools available for developers to aid with usability. It's important that the application doesn't contain too many views causing complication and increasing time usage. The design on the application will consist of a single page, containing a control screen and ESP32-Cam images. The control system will contain two buttons to open/close the door, with the backend functionality sending data to the ESP8266 via MQTT.

Although a security test will identify any potential issues within a website while it's being developed, literature review states the importance of authentication. Therefore, authentication via a login screen will be designed for this project. Most browsers offer automatic login to save time retyping credentials while visitors are waiting at the door. The login screen will be kept to a bare minimum in-terms of user design and will provide functionality that successful authentication directs users to the control panel page.

Authentication will be designed via PHP page which provides users to enter credentials stored in an SQL database. In real world application, these authentication details would be given with the smart home system on purchase. A graphical representation of the database could have been shown as part of this design, however, the database will only consist of one table and two entries, password and username.

4.3 Functional Requirements

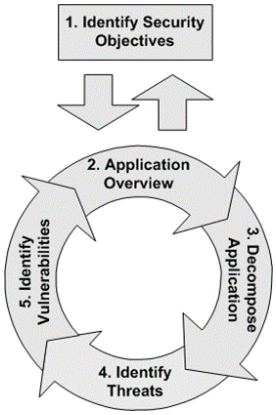
When reviewing the functional requirements for this project, the MoSCoW prioritization technique has been used. One of the main things considered is usability for individuals with disabilities and security issues, primarily expending on existing IoT smart-home devices.

ID	**MoSCoW**	**Functional Requirements**
M1	Must Have	Must be able to activate door with voice control
M2		Must have the ability to control the door physically
M3		Must be able to view who's currently at the door

M4		Must have the ability for the carer to enter through the door
M5		Must feature basic security
M6		Be able to access the door without an internet connection
S1	Should have	Application and/or website to control from outside the home
S2		View the current state of the door
S3		Sound to notify when someone has entered the building
S4		Basic Authentication
S5		Control from multiple devices in case one is down
S6		Be able to remove pictures from the website
C1	Could have	Central hub to view images of visitors
C2		LCD display and/or microphone to communication with visitors
C3		Push notification for which carer entered the property
C4		Two factor authentications for external application users
C5		Online framework to manage users
C6		Motion detection in case visitor doesn't press the doorbell
W1	Won't have (Future work)	Allow for multiple door control for care-home setting
W2		Allow access based on rooms in the house for privacy
W3		Built-in security system to notify when visitors enters property
W4		Custom images to be displayed depending on who enters the property

4.4 Security testing

When it comes to security testing it's important to keep the testing realistic and not test for every possibly outcome. The literature review outlined how easy it is for attackers to break into IoT devices and cause problems for organisation. Attacks are plentiful and if attackers gain data from the organisation it could become profitable. Many sophisticated attacks can take a great amount of time/preparation and attackers usually have a large amount of gain. Many simple attacks can be done in a couple of seconds but gain very little. When considering people with disabilities they can be extremely vulnerable if faced with an attacker, even against simple, whereas technology such as smart home also makes these individuals increasingly vulnerable. Rusell (2018), explains that when considering security threats within an IoT system, threat modelling must be designed. An overview of threat modelling is shown in the diagram below:



After conducting threat modelling, an evaluation must be done on our likely these attacks will occur. A complete attack spreading malware to infect the entire network is more likely to occur when considering unsecure systems within an organisation, however, such threats are highly unlikely for individual smart-home users.

Due to these reasons, after conducting threat modelling this project will focus on attacks that are likely to occur in smart-home devices. These are:

- Signal Jamming
- De-authentication attacks
- Information Gathering
- DDoS attack
- MITM attack
- RFID Cloner
- SQL Injection
- Reverse Engineering
- Spoofing

4.4.1 Security tools

Kali Linux features a range of security tools which can be used for penetration testing. Some of these devices are pre-installed on the operating systems, others are easily downloaded from sources such as GITHUB.

Aircrack-ng is used for signal jamming, de-authentication attacks, and information gathering. The software works with a wireless interface to scan a network and report back on any networks available in your local network.

HULK is an open software which overloads the HTTP request with traffic from devices. It's an open-source software which can be downloaded and easily installed onto the Kali operating system. This is a serious attack when considering IoT devices due to it being very easy to implement and can cause maximum damage.

Bettercap is used for man-in-the-middle (MITM) attacks and features tools to bypass HTTPS and HTSP websites. It's a very useful package, which can also be used with Wireshark to provide a GUI to analyse packets that have been captured. Bettercap also allows for DNS spoofing attacks, IP spoofing attacks, and email spoofing attacks.

4.5 Conclusion

The design was chosen based on current research outlined in the literature review. This provides an insight into a smart home system aimed at users with physical disabilities. Similar design techniques

can be used for larger-scale systems using the same technologies with one central control system. Therefore, the design section provides a useful insight into how a larger system can be designed by just expanding upon the proposed system.

Testing will be done on the system at each stage of development using the scrum methodology reviewed in early chapters. Any changes from the original design will be stated with reasonable explanations.

The website, android application, and physical system will be tested for security vulnerabilities and the changes will be implanted from the findings. Both website and application will be designed, developed, and tested on numerous occasions using the scrum methodology.

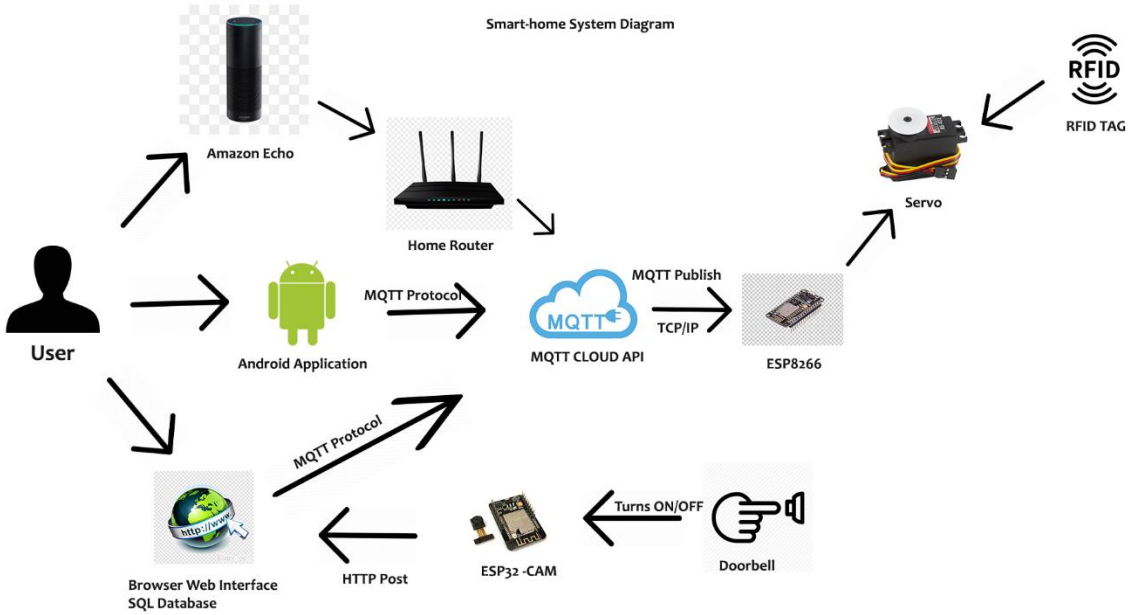
Due to numerous software (website, application) being developed for this project it's important that one aspect of the system is fully functional before moving onto the next. All features of the website must be performing adequately before the application can be developed. This is due to the application being dependant on the website's images.

Once the system is complete, testing will be done to try and break the system to identify any bugs or errors that the system may contain. It's important when considering people with disabilities that nothing can fail within the system once deployed.

5 Implementation

5.1 System Overview

A Smart Home diagram has been designed below to outline the main components of the system using a visual representation.



Most of the data has been sent via Message Queuing Telemetry Transport (MQTT) protocol which works on top of the TCP/IP protocol suite. The website interface, mobile application, and amazon echo notify the MQTT cloud server by sending publish commands which forwards onto the ESP8266 to open/close the door. MQTT protocol has been chosen for the main communication protocol within this project due to the capabilities of allow multiple gateways to send and receive data.

The HTTP protocol was also used to send images to from the ESP32-Cam in JSON format. This data is stored within a .PHP file on a web hosting platform (goDaddy). The doorbell acted as a switch to give power to the ESP32-Cam via a relay. The design chapter mentioned that a time for the relay to be activate would be dependent on the time it takes for the image to be uploaded via HTTP. This time for the relay was 13 seconds, which is approximately the time it takes for the image to be uploading with 100% success rate.

The RFID successful opened and closed the door when required. The code automatically closed the door after a brief delay to add physical security. This time was around three seconds, the typical door lock uses a latch-based system which would automatically lock the door; however, this feature was implemented for extra user functionality. RFID cards will be unique for each carer/resident entering the property. Although for simply outlining functionality only one RFID card has been used for successful entry, and another RFID card to test unsuccessful cards.

The review outlined how important cloud services was to the growing success of the IoT industry. It was therefore important that a cloud service was used within this project, more notably the MQTT cloud API. The MQTT cloud API was easy to implement with just a server address, username and password being required in the source code for successful connection.

5.2 Software Testing

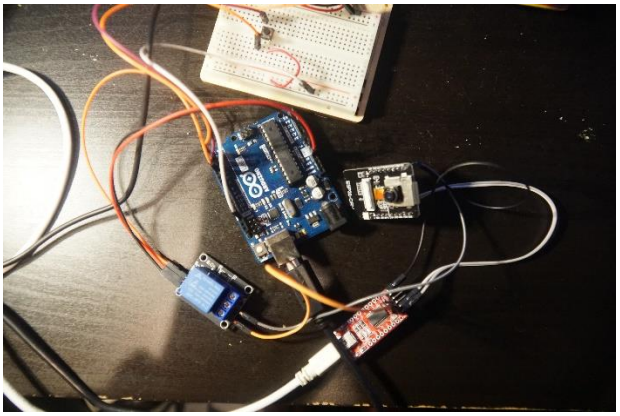
Each software and hardware component were tested while being designed using the scrum methodology to identify any bugs and/or errors. The code was developed during a sprint, with the end of each sprint contain software testing to identify any errors. At the end of each sprint an overview of the current system was identified. Any issues or changes required were noted and changed during the next sprint.

5.3 Resulting system

The main aim of the project was to design and develop a smart home system focussing on users with physical disabilities. The system would involve opening and closing a door using several devices such as mobile phone, computer, and voice assistant. It was important that this system used features tailored to those with physical disabilities. The literature review showed growing trends with developing products in relation to IoT and those with disabilities. Although reviews on smart homes have been conducted with disabilities in mind, no smart home specialises in products specifically for those with disabilities. It’s therefore important that this system reviewed the issues which need to be considered in making smart-home devices more disability friendly.

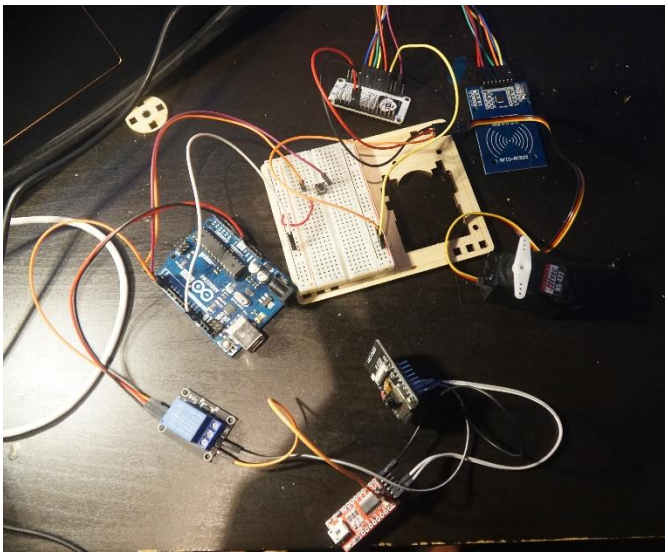
It was also of important that security issues were tested, and fixes implemented within such a system. The literature review highlighted the importance of cyber security and the growing threat of security issues within IoT devices.

One issue from faced from the design was the second circuit. It was found that using a pushbutton to control the power of the ESP-CAM resulted in failure. Further testing on this issue would be required to identify this problem. To solve the issue an Arduino board was used.



Once the Arduino board was added to the system it resulted in success.

The overall system resulted in no issues and was implemented as stated in the design section.



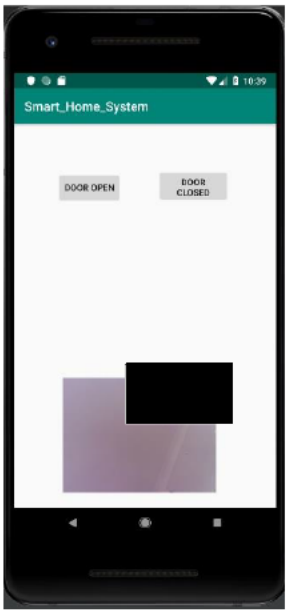
The above image shows the full system linked up. Due to the wires not being soldered onto the boards it's prove difficult to rearrange the system in an aesthetically pleasing way. However, all functionality within the system still performs successfully.

The full video of the working system can be found at the link provided – [redacted]).

5.3.1 Controlling the door via mobile application

The door can be successful controlled from four sources, an android application, a website interface, through the amazon Alexa, and using RFID tags. The android application allows for easy control of opening and closing the door via MQTT.

The android application can be demonstrated via Android Studio's phone emulator. Navigating the app is easy and is designed with users with disabilities in mind. The app allows user to check images of visitors at the door and allows them to choose whether to allow entry into the property. It was important that all this information was displayed on one page of the application to save time switching between views.



The image is loaded from the HTTP webpage using a String URL. The photo is shown directly from the website and not loaded onto on android application directly. It's therefore important that previous photos are deleted from the website to allow the application to display the most recent imagine.

5.3.2 Security issues with mobile application

An android application is arguable the most secure of all the entities within this project due to being harder to attack by nature. However, vulnerabilities are still plentiful within the application. It was important that the android application contained a username and password to enter the control view of the app. Without authentication anyone could possibly download the app and control the door.

An issue not tested within this project but worth a mention is reverse engineering on the application. Many deployed applications will not show source code for security and copyright reasons. However, certain tools such as Java decompilers could possibly access the source code which would allow full view of the MQTT cloud server details. This is one of the downfalls of having login details written in plain text on android studios.

5.3.3 Controlling the door via web interface

The website was built with usability in mind. Many users with disabilities may find having a tab open on their local system is an efficient way to control the system. After the first sprint cycle the website contain a page which could control the door via buttons. These buttons then sent MQTT data to the ESP8266. After security issues were tested between sprint cycles, the website included certain new features.

A PHP login screen is the first page that appears on the website, this then redirects to the control panel once successful authentication has been approved. The login screen sends an SQL query to the database to establish successful authentication. It was important not to over-engineering the website with security features which could implement the performance issues of the website.

The photos from the ESP32 are downloaded onto the onboard SSD card and uploaded via HTTP request to a PHP page. These photos can then be viewed via the website to identify which visitor is at the door.

The website can be seen at tombriggs.org. For viewing purposes access onto the authentication page can be seen at tombriggs.org/home. However, this website will only usually accessible via the login page.

5.3.4 Security Issues with Web Interface

After the first sprint the website had a basic control panel where users could open and close a door. Those with the URL would be able to access this, however, anyone who obtained the website address would be able to control the door. Therefore, it was important that basic authentication was needed to allow access to the control panel based.

A simple login was created to add authentication, however, this itself was not secure. After testing the login screen, it became clear that the website was still vulnerable. A simple SQL injection was ran on the login page which proved successful allowed access to the control panel. To fix this issue additional code was added to the project detailed below.

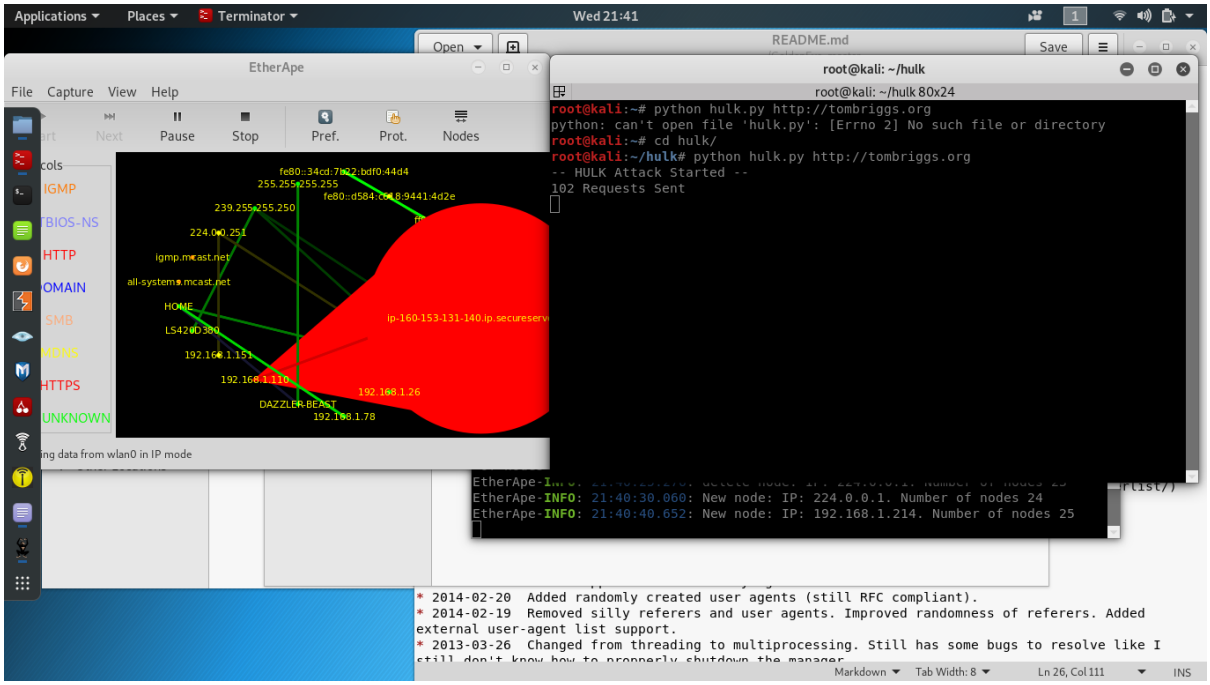
SQL injection attacks are very easy attacks to carry out and can be extremely dangerous when considering control over IoT devices. The positive of SQL injection attacks is the code is also relatively simple to implement. The code “1=1” typed into the username and password will be true, therefore allowing access to the database.

Secondly, a MITM attack was performed and provided a successful attack. The software bettercap was used to perform this attack and it allowed the attacker to see the username and password for the login screen. The main issue was the website uses HTTP and not the more secure HTTPS. This means all the packets that were sent to the internet were not encrypted, providing credentials to be seen in plain text. Although the website can be easily upgraded to HTTPS, HTTPS is also vulnerable to MITM attacks by spoofing another HTTP website, further steps can be spent trying to spoof the DNS if HTTP spoofing is unsuccessful. However, from the risk analysis this attack is highly unlikely due to the attacker not being able to gain much. Steps must still be taken to make it harder for an attacker to infect the system. Password hashing on the website is something which has been implemented to take extra steps in security. Infecting the IoT device with malware is something which is beyond the scope of this project, however, a simple JavaScript command embedded onto the website via a MITM attack is something which can be easily done.

The commands above shows how a MITM spoofing attack is easily implemented. This file is run with bettercap and attacks the device at IP address 192.168.1.22 on the network. The benefit of this script is you only have to change the IP address to perform the same attack again. This particular command spoofs the HTTPS addresses to HTTP.

A DDoS attack was carried out on the website which provide unsuccessful due to the hosting platform. For this project a popular hosting platform, goDaddy was used to host the website. However, not all IoT devices have secure hosting platforms and are vulnerable to a DDoS attack.

Although as inconvenient a DDoS attack would be on the project, in this case the system still has two additional sources to control the door in case of an attack.



Although the DDoS attack wasn't successful, you can see the attack working in the picture above. Using EtherApe installed on the Kali Linux operating system you can see the traffic on your local network. The green lines indicate normal traffic from one device to the network. It's clear to see how much traffic is being generated from the DDoS attack.

Although MITM attacks, Reverse Engineering, DDoS attacks are something which require at least some fundamental security knowledge, while building software to prevent such attacks it's easy to overlook simple vulnerabilities. The website's door control page is built using JavaScript and data sent to the MQTT cloud. One issue found within the project was the MQTT cloud credentials would be seen in plain text. Anyone can see this data by clicking F12 or CTRL+U, and copy the code into their own platform for them to control the door. It's therefore important that this code was hidden or removed. Obfuscating the code is one way to make the website more secure, however, with extra processing the details could still be obtained. Another way to fix this issue is to remove the code is to place it in another .js file and call the code.

5.3.5 Controlling the door via Amazon Alexa

The Amazon Echo is extremely useful when considering a smart home system which is tailored for users with physical disabilities. It provides a useful solution to control devices without the use of the limbs. Therefore, if a device was physically inaccessible for a user in a wheelchair, the Echo device provides an alternative.

The fauxmoESP library has been used to provide functionality to the amazon echo to control the device. The library emulates a Wemo Belkin device so save creating an Amazon Skill to perform the same task. FaxumoESP tracks the state of the door and sends data to the ESP8266. The useful feature of the Echo device is the ability to change the state of the ESP8266 to control the door. While the ESP8266 is programmed to track the state of the door, any changes via the Echo device will also send data via MQTT. Therefore, if the user had a central hub for example, it would be able to track the current state of the door from all four connect devices.

5.3.6 Security Issues with Amazon Alexa

Security testing issues with Amazon Echo can be more difficult than other devices, due to Amazon making sure the device is as secure as possible. However, some cyber attacks may affect the usage of the Echo. One thing noted was signal jamming and de-authentication attacks which affected the device greatly. Signal jamming attacks are mainly used to gain "hand-shakes" at an attempt to gain the network password, by jamming the signal to a user's local WiFi router. A phone that has been a victim of a jamming attack will take seconds to reconnect to the router once the attack as stopped. However, a problem with the Amazon Alexa is how effective the jamming attacks can be. When blocking the signal for the Alexa it took minutes instead of seconds to reconnect, sometimes hitting double figures in minutes to reconnect. When considering users trying to open or close a door, this is something which could be extremely frustrating. Although the attack is extremely unlikely due to attackers having very little to gain, it's still something which can be frustrating where an Echo device is concerned.

Although security standards at the basic level conserving the Amazon Echo are at a good level, many users may consider privacy a concern. The literature review outlines how many suspects that the amazon Alexa software constantly records and tracks data. This is something worth considering when using the amazon echo device.

5.3.7 Controlling the door via RFID

RFID has become popular throughout the years, with most people using RFID almost every day. This project used RFID to allow users access through the door. The RFID controls the servo and is program within Arduino. The servo automatically closes after 5 seconds to ensure physical security for the system.

This project was coded so that only certain users could get into the house to test for functionality. It's would be important that future work would allow users to modify and add users using RFID.

5.3.8 Security issues with RFID

The main security issue with RFID is RFID cloning. Many devices are on the market for only around £13 which can clone RFID cards. This device would allow attackers to gain the credentials to enter the property. The main prevention to this problem is RFID covers which block the cloning devices from access the details. However, many users could find this solution tiresome and not use the covers appropriately. A simpler prevention would be to educate users on RFID cloning issues and provide neck holders which many organisations have become accustom to.

6 Evaluation

The project provided an insight on how the system could control every aspect of the house. For users with disabilities the project provided many endpoints for them to comfortably control the system. Although the overall project was a success and the system were fully functional, a few changes could have been made the project more beneficial.

In the literature review and design, it was stated that the ESP devices will be used to control the system, detailing the benefits of being more energy-efficient and providing the same performance results. When developing the project, the use of the Arduino board was used to control the connected things. One proposed argument could be the use of a Raspberry-pi in this situation if an addition Arduino board is needed alongside an ESP32. Although the additional of an Arduino board provided more bulk to the project, the board only needed a small code implementation to become functional. Another benefit of the Arduino board being added to the system is the ability to control more than one relay or device. The Arduino board can provide much more performance capabilities than the ESP32. Furthermore, the ESP32 is used independently and can be placed almost anywhere providing adequate

cable length. Most raspberry-pi compatible cameras require connection onto the board. Although research suggested that the IPv6 communication protocol could be more power consuming than other protocols available, no issues were noted in the development of the project regarding this issue. In summary, the Arduino/ESP32 circuit still provided adequate benefits to justify the usage over the Raspberry-pi.

The mobile application used a simple yet effective view to showcase functionality to aid those with disabilities. However, the negative of the application is not having a push-notification when users are at the door. This makes the practicality of the application less useful if users are not located inside the house and used simply to check who has been entering the building. Although this feature would be simply enough to implement, it wasn't featured in this project due to timing reasons.

The website provided adequate functionality and security for users with physical disabilities. Although the website was useful, it could be argued that an application and website are both possibly not needed. Users outside of the property would most likely use a mobile application instead of the website. However, the project still proves insightful for developers that may only want to design and build one of these products. More preparation and planning of the project could have used the website for more practical functions. For example, the project would have been better suited having a website for management purposed e.g. the adding of RFID users, connecting new devices, viewing log reports. A mobile application could then be used for control purposes.

RFID cloning was an issue reported in the security testing done on the project. The website design mentioned above adding functionality to manage users would add another security element to such a system. Another potential idea would be the use of facial recognition within the project. This is something that was looked at in the project but was unsuccessful. One of the reasons was due to the system was getting to messy from safety aspect and overcomplicated. One of the limitations stated was the ESP32-CAM could only be used by one server at a time, meaning taking a picture and using facial recognition wouldn't be possible. A second ESP32-CAM device was tested within the project but wasn't successful implemented. Another workaround would be to save multiple images on the ESP32-CAM, with one getting uploaded to the website. The remaining images could be used with machine learning techniques for facial recognition. However, this was beyond the technical skills of the researcher and would have required more time.

6.1 Performance Results

Performance evaluation is essential for this project due to the nature of the system. If performance suffers than the time it takes to perform a certain task will increase. Certain individuals with disabilities will take an increased amount of time to access interfaces in comparison to other users. Therefore, if the system suffers performance issues then the overall time it takes to complete a task will increasingly tremendously.

The time it takes for an image to be uploaded from the ESP32 to HTTP is roughly 13 seconds. The ESP32-Cam saves the images captured from the web server stream and uploads it via HTTP. Once the doorbell is pressed it's possible that users could beat this 13 seconds upload time and may be frustrated having to refresh the page. However, for a user with disabilities 13 seconds seems to be an appropriate time to check the device. This time increases slightly when downloading the image onto the android application.

One thing taken into consideration when choosing which hardware components would be used was performance. The ESP32-Cam is a low-cost WIFI devices which can be easily implemented and performs adequate for the required task. Where performance may suffer is increasing the system to perhaps to a care-home environment. This would require more endpoints for the ESP-Cam to upload images. Alternative software such as the raspberry-pi comes with its own version of a camera, raspberry pi camera v2. which will perform slightly faster. This project uses the ESP32 with the

Arduino board to activate the camera. Switching to the raspberry-pi and Raspberry-pi V2 cam will result in a significant price increase. Although the Raspberry-pi system would perhaps contain higher quality images with faster upload speeds, the overall power consumption would greatly increase. For this reason, the low-cost solution, ESP32 still performs to an adequate performance for a single user with disabilities.

When reviewing communication protocols, it was decided that the project would use the MQTT protocol to send data to the cloud server. Performance and security issues were both noted, with MQTT proving to be the preferred protocol. The time it takes to send/retrieve data for the door to open is milliseconds. Although the time taken to control the door via MQTT is extremely fast, accuracy is sometimes amiss, this could be due to a network error or endpoint issues. One issue reported in the literature review was a limitation causing network traffic within IoT devices. Although opening the door is situational depending on the visitor, if multiple users were to send traffic it would usually be to perform the same task. It's therefore assumed that any data lost in traffic congestion would mean another use performed this action. Another issue which was faced was turning the door on by multiple devices, this would cause the servo to performance the same task twice. This causes the system to make a clunking noise until the door automatically closes. On occasions multiple presses of the same button can cause a prolonged duration for the door to close again.

One issue that was discussed in the literature review was error rate on voice recognition software. The Amazon Alexa performance was adequate for it's given task, however it still contained errors on occasions. Sometimes the command "Turn door on" would not be recognised which could cause frustrating and potential visitors could be turned away. In these situations, the application and website are useful to assist in such situations. However, until technology advancements on speech-recognition software improve this will be a common limitation.

Throughout all the performance testing, the system was tested on fast fibre-optic internet and the website/applications tested on high performance systems. Different possible outcomes may be presented if the system was testing on a range of technologies. A slower internet may affect the times it takes to upload data to a database. For these reasons it would be advised that a minimum hardware/software specification guideline are to be published if such systems were ever released. However, for this project it wasn't essential that testing was done on a multitude of devices.

6.2 Security issues

Previous sections outlined security issues that were found within certain sectors of the smart home system. Every different software/hardware entry provides a new gateway for hackers to target their attacks. The more complicated a system is, the more attack vectors they will be. It's important that these risks are minimized through the systems development.

Attacks like MITM, DDoS attack, SQL injection, Reverse engineering have already been mentioned. Most of these attacks can be targeted on the application or website, it's therefore important that all areas of the project are secure.

Within the overall system, security issues are also present. The research was able to use the ESP devices as gateways to capture handshakes for possible password breaches. Wireshark is a packet analysing software which was used to analyse data within this project. Without being connected to the local wireless router, it was still possible to see when the ESP devices were activated. Potential attackers can record the times the door is activated and prepare for any physical security attack. This issue is very hard to prevent due to the computation power many IoT devices. The IoT devices within this project are developed to perform a specific task. Therefore, onboard security software such as firewalls, anti-virus, malware detection is next to impossible. Future developments could potential see the increase of security solutions of IoT devices, however, this could then impact the overall performance of the system.

6.3 Usability

Usability was one of the key areas in this project. It was important that software within this project were developing with aid of helping those with physical disabilities. The website and android application minimised the need for extra, this was to save time navigating. It could take an extensive amount of time if a user has a slow system or a slow internet connection.

Although the application's GUI was developed using tools available through software. It's important when adding features such as custom buttons, background images, logos…to keep in mind design techniques for readability.

Although the fauxmoESP was a great library to use for providing functionality in controlling the servo via the Amazon Echo, the project could have benefited from extra features. These features could have been used if the project chose to develop an Alexa skill for the project. The features in mind could be to control the door based on specific timings. For example, if you know your deliver comes at the same time every day, a user can set this command up in the Amazon Echo.

A balance was needed within this project between usability and security. Sometimes having too much security could make the applications slower, require extra screens, and be overcomplicated. This project therefore focussed on the fundamental security issues which this system could face. However, a downside in making the system more friendly for users with disabilities is taking away things like secondary authentication.

7 Future Work

The project investigated how a smart home system can be used to aid a user with physical disabilities and an investigation into security issues within the device. The hardware used within this project can be used on a greater scale to develop a full smart home environment with one central control.

Future work on the project could be to research usability within all disabilities and not just physical disabilities. This would require a completely new application and website, although most of the hardware would stay the same. Many disabilities may require larger buttons and even voice control within the GUI.

An expansion from smart homes to smart systems for care homes could be another avenue for future work. This would require development to allow multiple users to control specific rooms within a building.

Although different smart home systems commercially available perform specific tasks, future research could look at ways to bridge these systems together. This could possibly be done by creating one application which can use features from many individual applications. Although the logistics of this solution may be possible, the legal issues within a system maybe an issue.

Future work in security and IoT systems continues to be a serious threat, especially when users with disabilities are considered. A review on how attacks could affect a range of disabilities would be beneficial. Many hobbyists are creating similar IoT devices for home and personal use. It would also be beneficial for future work to design an easy to use guide on how to protect such systems from attacks.

8 Future Trends

Future trends in IoT focussed on individuals with disabilities seems to be ending towards the use of AI. Smart-wheelchairs is a growing trend and with the evolution of smart-cars, it won't be long before smart wheelchairs are commercially available. Medical equipment and neural implants is another area

of interest within IoT research. While technology develops it's interesting to observe the role these technologies will play on smart homes.

Research into IoT and security is becoming more popular, with new frameworks and technologies being developed. Many researches are looking to find the happy medium between power consumption and IoT devices. Once this issue has been solved many IoT devices will contain more processing power which could allow for onboard security features.

9 Conclusion

Research in the area of IoT in relation to cyber-security issues and individuals with disabilities continues to grow. Currently many IoT smart home systems are commercially available on the market, however, no specific tailored smart home device takes into consideration the needs of users with disabilities. The term smart home usually relates to area of a building that can be controlled by sending/receiving data in some form of way e.g.…Smart door, smart lights, or smart plugs, with each node usually consists of individual applications or control panels.

To have the truly utopia "smart home" many different devices, brands, and technologies must be installed. For users with disabilities the use of several applications, websites, control panels etc... Is not only costly and tiresome but can become physically and mentally demanding beyond worth. This project therefore proposed a system with a review into certain technologies that could be developed into a complete smart home device controlling every aspect of the house.

It's also important that smart home systems are secure to prevent any cyber-attacks which may place individuals with disabilities at risk. This project aimed to test the potential system for any vulnerabilities that it may contain.

Overall the project demonstrated how the device used can be expanded to control the entire house. Several issues related to usability, potential performance issues, and device control from different gateways were identified. Further analysis showed how security issues can easily arise within IoT systems, with many issues being reported and the changes being implemented.

Overall the project resulted in a positive outcome, providing an insight into how a single device can control the entire house to aid those with disabilities. The project lays the foundation for future work to address certain problems and expand on the system.

9 References

Rouse, M. (2019). *What is network topology? - Definition from WhatIs.com*. [online] SearchNetworking. Available at: https://searchnetworking.techtarget.com/definition/network-topology [Accessed 28 Aug. 2019].

Lim, S., Kwon, O. and Lee, D. (2018). Technology convergence in the Internet of Things (IoT) startup ecosystem: A network analysis. *Telematics and Informatics*, 35(7), pp.1887-1899.

Vijayanandh, B. (2014). An Efficient Topology Search Mechanism for Unstructured PeerTo-Peer Networks. *IOSR Journal of Computer Engineering*, 16(3), pp.83-86.

LIN, X. and LEI, Z. (2008). Implementation of embedded IPv4/IPv6 dual-protocols stack. *Journal of Computer Applications*, 28(2), pp.406-408.

Alshahrani, M. and Traore, I. (2019). Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain. *Journal of Information Security and Applications*, 45, pp.156-175.

Byun, J., Jeon, B., Noh, J., Kim, Y. and Park, S. (2012). An intelligent self-adjusting sensor for smart home services based on ZigBee communications. *IEEE Transactions on Consumer Electronics*, 58(3), pp.794-802.

Shin, D., Sharma, V., Kim, J., Kwon, S. and You, I. (2017). Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks. *IEEE Access*, 5, pp.11100-11117.

Alshahrani, M. and Traore, I. (2019). Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain. *Journal of Information Security and Applications*, 45, pp.156-175.

Thuy Nga, D., Kim, M. and Kang, M. (2007). Delay-guaranteed Energy Saving Algorithm for the Delay-sensitive Applications in IEEE 802.16e Systems. *IEEE Transactions on Consumer Electronics*, 53(4), pp.1339-1347.

Badenhop, C., Graham, S., Ramsey, B., Mullins, B. and Mailloux, L. (2017). The Z-Wave routing protocol and its security implications. *Computers & Security*, 68, pp.112-129.

Ensworth, J. and Reynolds, M. (2017). BLE-Backscatter: Ultralow-Power IoT Nodes Compatible With Bluetooth 4.0 Low Energy (BLE) Smartphones and Tablets. *IEEE Transactions on Microwave Theory and Techniques*, 65(9), pp.3360-3368.

Wedd, M. (2019). *Bluetooth IoT Applications: From BLE to Mesh*. [online] IoT For All. Available at: https://www.iotforall.com/bluetooth-iot-applications/ [Accessed 28 Aug. 2019].

Goldberg, J. (2019). *IEEE 802.15.4-2015 - IEEE Standard for Low-Rate Wireless Networks*. [online] Standards.ieee.org. Available at: https://standards.ieee.org/standard/802_15_4-2015 html [Accessed 28 Aug. 2019].

Bhaskar, D. and Mallick, B. (2015). Performance Evaluation of MAC Protocol for IEEE 802. 11, 802. 11Ext. WLAN and IEEE 802. 15. 4 WPAN using NS-2. *International Journal of Computer Applications*, 119(16), pp.25-30.

Kološvari, A., Stojanović, R., Zupan, A., Semenkin, E., Stanovov, V., Kofjač, D. and Škraba, A. (2019). Speech-recognition cloud harvesting for improving the navigation of cyber-physical wheelchairs for disabled persons. *Microprocessors and Microsystems*, 69, pp.179-187.

Google Cloud. (2019). *Cloud Speech-to-Text - Speech Recognition | Cloud Speech-to-Text | Google Cloud*. [online] Available at: https://cloud.google.com/speech-to-text/ [Accessed 28 Aug. 2019].

Anggraini, N., Kurniawan, A., Wardhani, L. and Hakiem, N. (2018). Speech Recognition Application for the Speech Impaired using the Android-based Google Cloud Speech API. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 16(6), p.2733.

Amazon Web Services, Inc. (2019). *AWS Lambda – Serverless Compute - Amazon Web Services*. [online] Available at: https://aws.amazon.com/lambda/ [Accessed 28 Aug. 2019].

Ibm.com. (2019). *IBM Watson*. [online] Available at: https://www.ibm.com/watson [Accessed 28 Aug. 2019

Ibm.com. (2019). *Watson Natural Language Understanding*. [online] Available at: https://www.ibm.com/watson/services/natural-language-understanding/ [Accessed 28 Aug. 2019].

Rashid, Z., Melià-Seguí, J., Pous, R. and Peig, E. (2017). Using Augmented Reality and Internet of Things to improve accessibility of people with motor disabilities in the context of Smart Cities. *Future Generation Computer Systems*, 76, pp.248-261.

Škraba, A., Stojanović, R., Zupan, A., Kološvari, A. and Kofjač, D. (2015). Speech-controlled cloud-based wheelchair platform for disabled persons. *Microprocessors and Microsystems*, 39(8), pp.819-828.

Rvsn.csail.mit.edu. (2019). *Intelligent Wheelchair Project at MIT*. [online] Available at: http://rvsn.csail.mit.edu/wheelchair/ [Accessed 28 Aug. 2019].

Domingo, M. (2012). An overview of the Internet of Things for people with disabilities. *Journal of Network and Computer Applications*, 35(2), pp.584-596.

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

Rho, S. (2014). Analysis of RFID Standard Patent Data for RFID Technology Trends. *The Journal of Korea Navigation Institute*, 18(2), pp.185-190.

Bonsor, K. and Gadgets, H. (2019). *How RFID Works*. [online] HowStuffWorks. Available at: https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm [Accessed 28 Aug. 2019].

Abowd, G., Edwards, K. and Grinter, B. (2003). Smart homes or homes that smart?. *ACM SIGCHI Bulletin*, 2003, p.13.

Storey, K. (2010). Smart Houses and Smart Technology: Overview and Implications for Independent Living and Supported Living Services. *Intellectual and Developmental Disabilities*, 48(6), pp.464-469.

Sivaraman, V., Gharakheili, H., Fernandes, C., Clark, N. and Karliychuk, T. (2018). Smart IoT Devices in the Home: Security and Privacy Implications. *IEEE Technology and Society Magazine*, 37(2), pp.71-79.

Ali, B. and Awad, A. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors*, 18(3), p.817.

Lin, H. and Bergmann, N. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information*, 7(3), p.44.

Rosic, A. (2019). *What is Blockchain Technology? A Step-by-Step Guide For Beginners*. [online] Blockgeeks. Available at: https://blockgeeks.com/guides/what-is-blockchain-technology/ [Accessed 28 Aug. 2019].

Khan, M. and Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, pp.395-411.

Miloslavskaya, N. and Tolstoy, A. (2018). Internet of Things: information security challenges and solutions. *Cluster Computing*, 22(1), pp.103-119.

Malviya, H. (2016). How Blockchain Will Defend IOT. *SSRN Electronic Journal*.

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, 54, pp.1-31.

CAI, Z. (2008). New research about covering communication based on protocol of IPSec over DNS. *Journal of Computer Applications*, 28(7), pp.1786-1788.

Alotaibi, B. and Elleithy, K. (2016). A New MAC Address Spoofing Detection Technique Based on Random Forests. *Sensors*, 16(3), p.281.

Shin, D., Sharma, V., Kim, J., Kwon, S. and You, I. (2017). Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks. *IEEE Access*, 5, pp.11100-11117.

Madhugundu, D., Ahmed, F. and Roy, B. (2018). A Survey on Security Issues and Challenges in IoT Based Smart Home. *SSRN Electronic Journal*.

Westerlund, O. (2019). Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things. *019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*, 1(10).

Mansfield-Devine, S. (2011). DDoS: threats and mitigation. *Network Security*, 2011(12), pp.5-12.

Reddy, V. and Nirmala, M. (2016). Spoofing Attack Detection And Localization In Wireless Networks. *International Journal Of Engineering And Computer Science*.

Li, C., Qin, Z., Novak, E. and Li, Q. (2017). Securing SDN Infrastructure of IoT–Fog Networks From MitM Attacks. *IEEE Internet of Things Journal*, 4(5), pp.1156-1164.

Ceron, J., Steding-Jessen, K., Hoepers, C., Granville, L. and Margi, C. (2019). Improving IoT Botnet Investigation Using an Adaptive Network Layer. *Sensors*, 19(3), p.727.

Kh, R. (2017). Ransomware and IoT among leading threats. *Network Security*, 2017(9), p.2.

Alshahrani, M. and Traore, I. (2019). Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain. *Journal of Information Security and Applications*, 45, pp.156-175.

Moos, J. (2017). IoT, Malware and Security. *ITNOW*, 59(1), pp.28-29.

Knoll, L. (2019). *Council Post: Developing The Connected World Of 2018 And Beyond*. [online] Forbes.com. Available at: https://www.forbes.com/sites/forbestechcouncil/2018/03/16/developing-the-connected-world-of-2018-and-beyond/ [Accessed 29 Aug. 2019].

Madakam, S. (2015). Internet of Things: Smart Things. *International Journal of Future Computer and Communication*, 4(4), pp.250-253.

Firth, N., Harding, E., Sullivan, M., Crutch, S. and Alexander, D. (2018). ECHOES AROUND THE HOME: CAN THE AMAZON ECHO BE USED IN THE HOME TO HELP THOSE LIVING WITH DEMENTIA?. *Alzheimer's & Dementia*, 14(7), pp.P184-P185.

Chung, H., Park, J. and Lee, S. (2017). Digital forensic approaches for Amazon Alexa ecosystem. *Digital Investigation*, 22, pp.S15-S25.

Developer.amazon.com. (2019). *Request and Response JSON Reference | Alexa Skills Kit*. [online] Available at: https://developer.amazon.com/docs/custom-skills/request-and-response-json-reference html [Accessed 29 Aug. 2019].

Zakariyya, S. (2017). Design of a Bimodal Home Automation System using ESP8266 and ATMEGA328 Microcontroller. *Computer Engineering and Applications Journal*, 6(3), pp.95-108.

Hutabarat, D., Budijono, S. and Saleh, R. (2018). Development of home security system using ESP8266 and android smartphone as the monitoring tool. *IOP Conference Series: Earth and Environmental Science*, 195, p.012065.

Sihombing, P., Manullang, M., Sitompul, D. and Sri Dumayanti, I. (2019). The Heart Attack Detection by ESP8266 Data Communication at a Real Time to Avoid Sudden Death. *Journal of Physics: Conference Series*, 1235, p.012044.

Firmansyah, R., Widodo, A., Romadhon, A., Hudha, M., Saputra, P. and Lestari, N. (2019). The prototype of infant incubator monitoring system based on the internet of things using NodeMCU ESP8266. *Journal of Physics: Conference Series*, 1171, p.012015.

Amazon Web Services, Inc. (2019). *What is AWS*. [online] Available at: https://aws.amazon.com/what-is-aws/ [Accessed 29 Aug. 2019].

Park, J., Kim, H. and Kim, W. (2018). DM-MQTT: An Efficient MQTT Based on SDN Multicast for Massive IoT Communications. *Sensors*, 18(9), p.3071.

A. P., H. and K., K. (2019). Secure-MQTT: an efficien,t fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. *EURASIP Journal on Wireless Communications and Networking*, 2019(1).

Zigbee Alliance. (2019). *What is Zigbee?*. [online] Available at: https://zigbee.org/what-is-zigbee/ [Accessed 29 Aug. 2019].

process, T., Journal!, A., You, H. and Lockers, T. (2019). *What is RFID and How Does RFID Work? - AB&R®*. [online] AB&R. Available at: https://www.abr.com/what-is-rfid-how-does-rfid-work/ [Accessed 29 Aug. 2019].

Serpanos, D. and Papalambrou, A. (2008). Security and Privacy in Distributed Smart Cameras. *Proceedings of the IEEE*, 96(10), pp.1678-1687.

Hao, P., Wang, X. and Shen, W. (2018). A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication. *IEEE Access*, 6, pp.42279-42293.

Yoo, S. (2014). Two-Phase Malicious Web Page Detection Scheme Using Misuse and Anomaly Detection. *International Journal of Reliable Information and Assurance*, 2(1), pp.1-10.

M.Kom, S. (2016). DATA COMMUNICATION ANALYSIS WITH XML AND JSON ON WEBSERVICE. *Computer Engineering, Science and System Journal*, 1(2), pp.1-6.

Buchanan, W., Helme, S. and Woodward, A. (2018). Analysis of the adoption of security headers in HTTP. *IET Information Security*, 12(2), pp.118-126.

Musliyana, Z., Dwipayana, M., Helinda, A. and Maizi, Z. (2018). Improvement of Data Exchange Security on HTTP using Client-side Encryption. *Journal of Physics: Conference Series*, 1019, p.012073.

Vijayasarathy, L. and Butler, C. (2016) 'Choice of Software Development Methodologies: Do Organizational, Project, and Team Characteristics Matter?'. *IEEE Software*, 33(5) pp.86-94.

Appendix A : Terms of Reference (TOR)

Project Title

NW.17 – A practical Security Testing of IoT Devices in a Smart House Environment

Project Background

The term Internet of Things (IoT) is used to describe devices that are essentially connected to the internet. However, with the growing trend of IoT the term is used as more of a relation between devices which can "talk" to each other using the internet. These devices are usually linked up to form a system, which can range from low-powered sensors to smartphones or personal computers. The popularity of IoT has increased over the past few years, in 2018, 7 billion devices were connected to the internet. This figure is set to rise according to the Gartner Report, with the number of devices connected across all technologies will reach 20.6 billion by 2020. With such a rapid growth rate, IoT is becoming a forefront to solving some of the worlds biggest problems.

Devices such as the amazon echo, google home, and other personal assistants are becoming used more in everyday life. These devices are now becoming known as "smart homes" due to their capabilities to control and talk to other devices (IoT) within a user's home. Things like, security cameras, lightbulbs, thermostats, kettles, can all be controlled using voice commands with a personal assistant. The main benefit of these IoT devices is that they provide ease of use for users, with a lot of IoT being linked up with mobile applications to control systems from outside of the house.

With the advances of IoT, not only has it made everyday life more convenient for everyday users, but IoT has made life a lot easier for people with disabilities. IoT allows users with disabilities to change aspects of the physical world from within the digital world. A study looked at an overview of the IoT for people with disabilities and believed that IoT can offer people with disabilities the assistance and support they need to achieve a greater quality of life. Research has already been done for people who are physically impaired to see how IoT can improve the quality of their life, all reporting positive outcomes. Body sensors and actuators have been used to detect user's intention to move certain muscles. Smart home systems have been used with mobile applications to allow disabled users to control home appliances. Further research is also being conducted to allow the IoT to help users with disabilities conduct online shopping. With the increasing popularity and developments of IoT, more people with disabilities will be able more independent due to IoT.

Although the advancements of IoT comes with many positives, the negatives of IoT should not be overlooked. The security threat that comes with IoT should be taken serious by all users of IoT devices, whether personal or organisational users. Research conducted earlier this year revealed that many organisations lack the skills to develop, manage and deploy IoT solutions, especially in the areas of data analytics and cyber security. One of the biggest challenges of IoT is to ensure data a privacy is protected. Hackers have already started targeting IoT devices, most recently on baby monitors. With IoT usually consisting of low powered sensors, mobile communication, and near constant access to the internet, hackers are targeting these devices to spread malware throughout the networks.

This project will combine aspect of IoT, security, and disability usability to create a smart house environment suitable for a user with physical impairments. The project will then investigate security issues with such environments. All issues found will be reported on and the required changes will be implemented. This project was chosen due to an interest in cyber-security and IoT, particularly in relation to helping those with disabilities.

Project Aims

To design and develop a smart house environment suitable for users with physical impairments. A further investigation into security and privacy issues within a smart house environment, with implementation of potential issues.

Project Objectives

- Write a literature review on the following areas: Smart house environments, IoT in relation to disabilities, Security issues within an IoT house environment.
- Analysis and review the laws and ethics, in areas specific to security and users with disabilities.

Department of Computing and Mathematics Computing and Digital Technology Postgraduate Programmes Terms of Reference Coversheet	
Student name:	[redacted]
University I.D.:	
Academic supervisor:	Nick Whittaker
External collaborator (optional):	
Project title:	NW.17 – A practical Security Testing of IoT Devices in a Smart House Environment
Degree title:	MSc Computing
Project unit code:	6G7Z10SS
Credit rating:	60
Start date:	27/05/2019
ToR date:	14/06/2019
Intended submission date:	27/09/2019
Signature and date student:	[redacted]
Signature and date external collaborator (if involved):	

1

- Review the range of specific hardware and software for such environments, API's commonly used in IoT projects, databases used.
- Design the smart house environment, show components used in the design, show relationships between each component and the link to devices.
- Implement the design in developing the system using appropriate API's, cloud servers, and applications.
- Write an initial report outlining any security issues with the system, compare the security with other IoT security research.
- Implement the changes needed to make the system more secure.
- Critically evaluate the system, compare to current research and other IoT devices. Report upon reliability, ease of use, and practically of the system.

Hardware Required –

- Phidgets
- Laptop
- WiFi Adapter compatibility for security
- Amazon Echo
- Raspberry Pi
- Android Smart Phone
- Raspberry Pi Camera V2
- ESP8266 WiFi Module

Software Required –

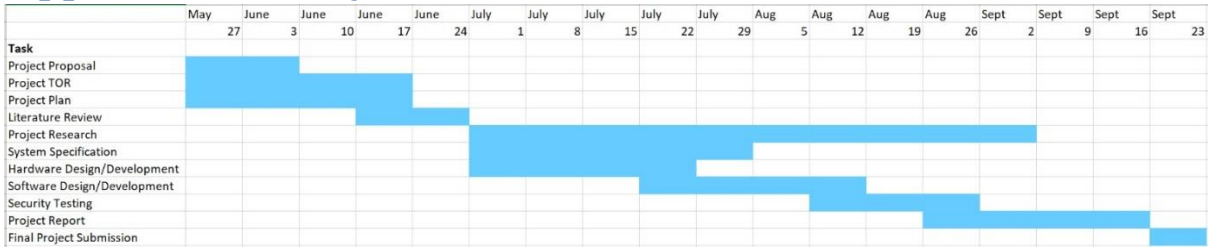
- Linux OS (VM)
- Android Studios
- MQTT
- Alexa Skills
- Phidgets Toolkit
- Java Development Kit

Project Deliverables –

- Project Proposal
- Project TOR
- Project Plan
- Literature Review
- System Specification
- Hardware design and development
- Software design and development
- Security testing and implementation
- Project Report
- Project Submission

Project Plan

Appendix B – Project Timeline



Appendix C – Project Code

Dropbox Link to project files -

[redacted]