|  |  |
| --- | --- |
| gcu logo color | **MSc Dissertation proposal** |

|  |  |
| --- | --- |
| MSc Programme Name: | MSc Big Data Technologies |
| Student Name: | Christopher Dillon |
| Student Matriculation Number: | S1514278 |
| Title of the proposal: | Development of a Secure Raspberry Pi Based Home Surveillance System |
| Dates submitted: [Please keep all dates of submissions and revised proposal submissions] | 10/06/2019, Revised 14/06/2019, Final Revision 17/06/2019 |
| Member(s) of academic staff that proposal has been discussed with: | Dr Anna Lito Michala |
| Agreed Supervisor Name: | Dr Anna Lito Michala |
| This proposal is my own original work and has not been submitted elsewhere in fulfilment of the requirements of this or any other award. | |
| Student Signature: | Christopher Dillon |

Table of Contents

[1.0 Introduction 3](#_Toc11673643)

[1.1 Background 3](#_Toc11673644)

[1.2 Problem Description 4](#_Toc11673645)

[2.0 Project objectives 5](#_Toc11673646)

[2.1 Project aim & objectives 5](#_Toc11673647)

[2.2 Project’s milestones and deliverables 5](#_Toc11673648)

[3.0 Technical Method of Proposed Project 6](#_Toc11673649)

[3.1 Proposed Software 6](#_Toc11673650)

[3.1.1 Face Recognition Technology 6](#_Toc11673651)

[3.1.2 Application Development 6](#_Toc11673652)

[3.2 IoT Architecture 6](#_Toc11673653)

[3.2.1 Perception Layer 6](#_Toc11673654)

[3.2.2 Network Layer 7](#_Toc11673655)

[3.2.3 Application Layer 7](#_Toc11673656)

[3.3 Common Attacks on IoT Devices 7](#_Toc11673657)

[3.3.1 DOS Attack 7](#_Toc11673658)

[3.3.2 Man in The Middle Attack 7](#_Toc11673659)

[3.3.3 Malicious Code Attack 7](#_Toc11673660)

[3.4 Network Layer Protocols 8](#_Toc11673661)

[3.4.1 Bluetooth 8](#_Toc11673662)

[3.4.2 Wi-Fi 8](#_Toc11673663)

[3.5 Application Layer Protocols 8](#_Toc11673664)

[3.5.1 Message Queue Telemetry Transport 8](#_Toc11673665)

[3.5.2 Advance Message Queueing Protocol 8](#_Toc11673666)

[3.5.3 Extensible Messaging and Presence Protocol 8](#_Toc11673667)

[4.0 Project Risk Management Strategy 9](#_Toc11673668)

[5.0 References 10](#_Toc11673669)

# 1.0 Introduction

## 1.1 Background

Smart security is growing at an exponential rate with an expected revenue forecast of 28 million by the end of 2023 as shown in Figure 1. Although such technology poses many advantages over traditional non-internet based security, cybersecurity has been a rising concern with small IoT based devices. This is concerning enough that the UK Government poses to introduce new legislation based on Internet of Things (IoT) security, requiring products to pass security requirements before being sold and introducing mandatory labelling schemes for each product, showing how secure they are (Ashford, 2019). This is further highlighted with recent media scares such as baby monitors being hacked with the hacker being able to speak through the baby monitor and threatening the parents (Wang, 2018).

With mainstream IoT devices being consistently hosted on the cloud, this offers individuals with malicious intent another method in taking down or accessing IoT devices. Recently, Google Cloud, one of the cloud vendor giants was taken down in a possible cyber-attack (Merriman, 2019), highlighting the potentially unreliability of Cloud hosted services. Organisations that depended on Googles Cloud, including security company Nest had their services taken down for over 4 hours. This is problematic in an area such as face-recognition based CCTV, meaning if data cannot be accessed from the Cloud, the whole system could break.

To limit the scope of potential security vulnerabilities, a locally stored Raspberry Pi based security system has been proposed. Presently, there are many people opting for Raspberry Pi smart systems at home due to the flexibility and cost of the Raspberry Pi. This, as with all Internet of Things devices, has many security flaws which are easily exploitable by those with malicious intent. Offering set guidelines and covering every layer of IoT architecture can present a model to base future systems on and prevent these cyber-attacks.

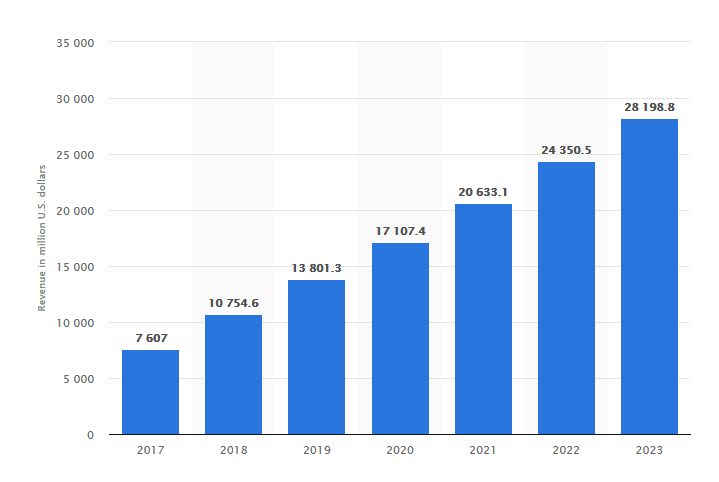


Figure 1: Smart Home - revenue forecast for the segment Security worldwide\* from 2017 to 2023 (in million U.S. dollars) (source: www.statista.com)

## 1.2 Problem Description

Modern IoT-based security systems pose various security risks to the individual. With the majority of these services using cloud technology, there is a larger scope of security concerns covering the full system stack. The development of a home security system using a Raspberry Pi model is proposed to create a system with a smaller scope of security vulnerabilities using local data storage to reduce information exposure over the system. The Raspberry Pi will interact with a smart phone app, with each family member having access to the application. This means security can be focused down to the perception, network and application layers of the IoT architecture.

This project aims to tackle the following areas of security:

* Authorised access to the Raspberry Pi (authentication)
* Integrated authentication for the smart phone app and IoT platform
* Explore security through restricting port access
* Storage security through encryption and reducing exposure of data to the network

These will be created in accordance with the best practices outlined by the IoT security foundation (IoT Security Compliance Framework, 2018). If time permits, a separate machine can be set up with the Kali Linux operating system, an operating system used in cyber security and digital forensics. The machine can perform various cyber-attacks (sniffing, MITM, DoS) and evaluate how the system performs against them. A recent paper demonstrates various types of DoS attacks were carried out in a test bed environment against an IoT device, resulting in a success attack against the network it was hosted on (Liang et al., 2016).

# 2.0 Project objectives

## 2.1 Project aim & objectives

This project aims to achieve the following objectives:

* Review state of the art literature for a home surveillance system. It is important to determine methods in recognising who is entering the premises whether it be a family member or a complete stranger
* Determine best security practices at all levels of the IoT architecture
* Creation of the interconnected physical system (Raspberry Pi, camera, sensors, smart app development etc.)
* Development of relevant scripts with proposed technologies integrated
* Development of a smart phone application that interacts with the Raspberry Pi/Security system
* Test performance versus security level for the proposed system
* Set up test bed, used for simulating attacks on the system
* Conclude results/findings

## 2.2 Project’s milestones and deliverables

* Best practices are determined through development of the literature review
* System design/proposed methodology is determined using knowledge gathered from previous stage
* Completed development of system
* Testing and evaluation report of the system
* Conclusion & final report write up

# 3.0 Technical Method of Proposed Project

The proposed system is a home security system using the Raspberry Pi as the core component. The system would be able to detect individuals faces entering the premises and inform the family members if a face was not recognised via app notification. As with all IoT based devices, the Raspberry Pi poses multiple security risks at the Perception, Network and Application levels.

The proposed hardware for this system would be a Raspberry Pi 3 and one or multiple cameras placed near the vicinity of the home entrance. Although simplistic, a similar system was used for border surveillance and shown successful (Abdalla and Veeramanikandasamy, 2017).

## 3.1 Proposed Software

### 3.1.1 Face Recognition Technology

OpenCV is an open source that offers a range of feature detecting and feature matching algorithms. It is shown that the majority of the algorithms used, detect thousands of features with seconds (Noble, 2016), making it suitable for a face detection system. To highlight the accuracy of this technology, a recent paper showed success in detecting eye fatigue in drivers using OpenCV (Manoharan and Chandrakala, 2015).

### 3.1.2 Application Development

To allow a family member receive an image and notification of who is at the door, a smart phone application has been proposed. A recent 2018 paper showed a similar system using image notifications from a Raspberry Pi Camera sent via email when a potential intruder was located at their door (Pawar and Umale, 2018). Although successful this mode of delivery is problematic security wise. With a service such as email being susceptible to PC security risks such as viruses, Trojans, a smart phone app is suggested to mitigate these potential threats. Using an app poses the advantage of 2-way authentication and security risks being limited to the scope of a mobile phone, rather than an email service which can be accessed anywhere.

## 3.2 IoT Architecture

IoT security faces three levels of architecture that can be attacked with malicious intent. As detailed in a recent 2018 paper, the most basic agreed upon architecture consists of three layers: Perception Layer, Network Layer and Application Layer (Aziz and Haq, 2018).

### 3.2.1 Perception Layer

This layer consists of the physical sensors which collect information and identify objects. Commonly used sensors include RFID, barcode & cameras. In this experiment the security camera is the main focus of this layer and can pose multiple potential security issues. As highlighted in the article mentioned previously, eavesdropping is definitely the most concerning security issue in this layer. Having unauthorised access to video footage is a serious breach of privacy. This is accomplished by taking advantage of insecure modes of transmission, granting access to a third party without authorisation.

### 3.2.2 Network Layer

The network layer is responsible for the transmission of data, acting as a sort of bridge between the perception and application layer. This involves carrying and transmitting information using through a wireless network which poses a set of security challenges. The layer acts as a sort of Central Nervous System for the whole network. In this scenario, the network layer consists of a standard wireless home network.

### 3.2.3 Application Layer

This layer is used to define all applications that use IoT technology. Common examples of this layer include smart homes, smart cities, smart health etc. This layer utilises the data gained from the previous layers and allows the user to use the application and enjoy its benefits. In this experiment the application layer would consist of the smart phone app used to operate the door and receive images/information from the security camera.

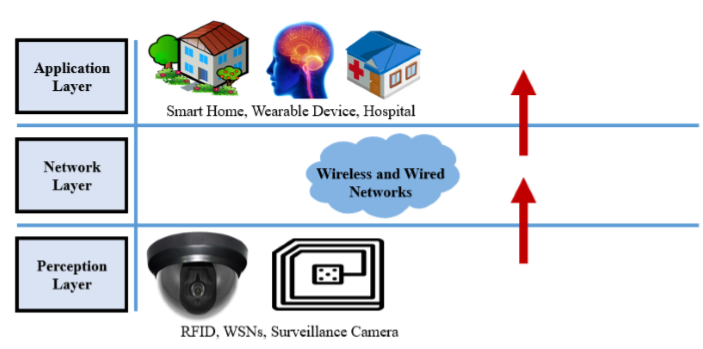


Figure : The basic three layered architecture of IoT Devices (Burhan et al., 2018)

## 3.3 Common Attacks on IoT Devices

### 3.3.1 DOS Attack

Denial of Service attacks are used to prevent access to devices or network resources, essentially taking the network offline. It is accomplished by flooding a network with packets and redundant requests to the point of the network being unable to be accessed by authentic users (Prabhakar, 2017).

### 3.3.2 Man in The Middle Attack

The man-in-the-middle has the ability to capture all messages between a server and IoT device via network spoofing. Using this spoofing strategy, it can assume identification of both the IoT device and server and trick both devices into believing they are still communicating with each other (Conti, Dragoni and Lesyk, 2016).

### 3.3.3 Malicious Code Attack

This is code in any part of the software intended to cause undesirable effects and potentially causing the system to malfunction. This cannot be detected by security tools such as anti-viruses as it not detected as a virus or malware.

## 3.4 Network Layer Protocols

### 3.4.1 Bluetooth

Bluetooth is used to communicate between two devices within a short distance. It provides a layer of encryption by converting a message or data into cipher text before sending it to the receiver device. This message, cannot be understood by other devices except those which have the rights to see the message. The sender must always get permission rights from the receiving device before the message can be sent. This is done through the sender device requesting permission to send data to the received device, once agreed to, the devices can then communicate within the short distance.

### 3.4.2 Wi-Fi

Wi-Fi is a wireless communication network that transmits communication in the form of radio signalling. This is the most common type of communication used in modern homes which is problematic as it provides multiple security vulnerabilities. The main issue being, by default, there is no encryption mechanism. This leaves the network prone to MITM attacks, sniffing etc. It is well documented that Wi-Fi is one of the most commonly used network protocols in smart homes (Alam, Reaz and Ali, 2012).

3.4.3 Radio Frequency Identification

RFID utilises frequency waves to establish communication between two devices. It usually consists of three parts: the tags, reader and a database. Unfortunately, there is no security when reading information from tags, meaning anyone with access to a tag would be able to use it without verification. This inherently, makes it insecure, as there is no way of identifying if someone is who they say they are.

## 3.5 Application Layer Protocols

### 3.5.1 Message Queue Telemetry Transport

MQTT is the most commonly used application layer protocol, being light weight and using a publish-subscribe model. The protocol is mainly used where a small code footprint is required i.e. sensor data and where bandwidth is limited. With the maximum amount of data being transferred 256MB (Rastovich, 2015), speed is the priority with this protocol.

### 3.5.2 Advance Message Queueing Protocol

AMQP is an open standard application layer protocol for middleware messaging. It has additional features such as message orientation, switching, reliability and queueing. Both point-to-point and publisher subscriber models are available with this protocol.

### 3.5.3 Extensible Messaging and Presence Protocol

XMPP was created with the intention of being used for real time communication and streaming of XML between networks. It is broader in terms of its capabilities, including being applicable in gaming, party chatting, video calling and messaging.

# 4.0 Project Risk Management Strategy

This project has multiple potential risks due to the time constraint of 3 months for completion. As multiple components are required for this project there could be potential delays in delivery of components. To mitigate this, components required have been orders weeks in advance before the actual development stage of the dissertation. An additional Raspberry Pi has been ordered in the slight chance the original malfunctions mid-way through the project. A contingency allowance of one week has been allocated to prepare in advance for any unexpected event or illness.

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Risk Level | Steps to Address Risk | Resulting Risk Level |
| Illness | High | A contingency allowance of one week has been allocated | Medium |
| Delays in component ordering | High | Components have been ordered weeks in advance | Low |
| Components breaking/malfunctioning | High | Replacement components have been ordered in advance | Low |
| Unexpected event | Medium | A contingency allowance of one week has been allocated | Low |
| Supervisor Unavailable | Medium | Schedule meetings in advance and replacement meetings if something unexpected comes up | Low |
| Work progress loss | Medium | Use of version control system such as git and the university storage to automate back-ups of written work | Low |

# 5.0 References

1. Merriman, C. (2019). *Google Cloud burst downs G Suite, Nest and Snapchat during 4-hour outage | TheINQUIRER*. [online] http://www.theinquirer.net. Available at: https://www.theinquirer.net/inquirer/news/3076657/google-cloud-outage [Accessed 7 Jun. 2019].
2. Wang, A. (2018). ‘I’m in your baby’s room’: A hacker took over a baby monitor and broadcast threats, parents say. [online] Washington Post. Available at: https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/?noredirect=on&utm\_term=.04321c476652 [Accessed 7 Jun. 2019].
3. Ashford, W. (2019). *UK gears up for new laws on IoT security*. [online] ComputerWeekly.com. Available at: https://www.computerweekly.com/news/252462505/UK-gears-up-for-new-laws-on-IoT-security [Accessed 7 Jun. 2019].
4. Aziz, T. and Haq, E. (2018). Security Challenges Facing IoT Layers and its Protective Measures. *International Journal of Computer Applications*, [online] 179(27), pp.31-35. Available at: https://www.researchgate.net/publication/323892938\_Security\_Challenges\_Facing\_IoT\_Layers\_and\_its\_Protective\_Measures [Accessed 9 Jun. 2019].
5. Prabhakar, S. (2017). NETWORK SECURITY IN DIGITALIZATION: ATTACKS AND DEFENCE. *INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS*, [online] Vol. 5 Issue 5(ISSN 2320-7345). Available at: https://www.ijrcar.com/Volume\_5\_Issue\_5/v5i512.pdf [Accessed 9 Jun. 2019].
6. Conti, M., Dragoni, N. and Lesyk, V. (2016). A Survey of Man In The Middle Attacks. *IEEE Communications Surveys & Tutorials*, [online] 18(3), pp.2027-2051. Available at: https://ieeexplore.ieee.org/document/7442758 [Accessed 9 Jun. 2019].
7. Burhan, M., Rehman, R., Khan, B. and Kim, B. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors*, [online] 18(9), p.2796. Available at: https://www.researchgate.net/publication/327272757\_IoT\_Elements\_Layered\_Architectures\_and\_Security\_Issues\_A\_Comprehensive\_Survey [Accessed 9 Jun. 2019].
8. Noble, F. (2016). Comparison of OpenCV's feature detectors and feature matchers. *2016 23rd International Conference on Mechatronics and Machine Vision in Practice (M2VIP)*. [online] Available at: https://ieeexplore.ieee.org/document/7827292 [Accessed 26 May 2019].
9. Diachok, R., Dunets, R. and Klym, H. (2018). System of detection and scanning bar codes from Raspberry Pi web camera. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. [online] Available at: https://ieeexplore.ieee.org/document/8409124 [Accessed 26 May 2019].
10. Abdalla, G. and Veeramanikandasamy, T. (2017). Implementation of spy robot for a surveillance system using Internet protocol of Raspberry Pi. *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. [online] Available at: https://ieeexplore.ieee.org/document/8256563 [Accessed 26 May 2019].
11. Alam, M., Reaz, M. and Ali, M. (2012). A Review of Smart Homes—Past, Present, and Future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, [online] 42(6), pp.1190-1203. Available at: https://ieeexplore.ieee.org/document/6177682 [Accessed 9 Jun. 2019].
12. Pawar, A. and Umale, V. (2018). Internet of Things Based Home Security Using Raspberry Pi. *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*. [online] Available at: https://ieeexplore.ieee.org/document/8697345 [Accessed 9 Jun. 2019].
13. Manoharan, R. and Chandrakala, S. (2015). Android OpenCV based effective driver fatigue and distraction monitoring system. *2015 International Conference on Computing and Communications Technologies (ICCCT)*. [online] Available at: https://ieeexplore.ieee.org/document/7292757 [Accessed 10 Jun. 2019].
14. Rastovich, R. (2015). *Why the MQTT Protocol is Ideal for the Internet of Things – ThingLogix, Inc*. [online] Thinglogix.com. Available at: https://www.thinglogix.com/why-the-mqtt-protocol-is-ideal/ [Accessed 10 Jun. 2019].
15. Liang, L., Zheng, K., Sheng, Q. and Huang, X. (2016). A Denial of Service Attack Method for an IoT System. *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*. [online] Available at: https://ieeexplore.ieee.org/document/7976501 [Accessed 12 Jun. 2019].
16. IoT Security Compliance Framework. (2018). [ebook] Available at: https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf [Accessed 17 Jun. 2019].