

**Development of a Secure Raspberry Pi Based Home Surveillance System**

Design Report

Christopher Dillon

S1514278

**“Except where explicitly stated, all work in this report, including the appendices, is my own original work and has not been submitted elsewhere in fulfilment of the requirement of this or any other award”**

**Signed: Christopher Dillon Date:19/07/19**

Table of Contents

[1.0 Introduction 6](#_Toc14464793)

[1.1 Background 6](#_Toc14464794)

[1.2 Problem Description 7](#_Toc14464795)

[1.3 Project objectives 8](#_Toc14464796)

[2.0 Literature Review 9](#_Toc14464797)

[2.1 Internet of Things Architecture 9](#_Toc14464798)

[2.1.1 Perception Layer 9](#_Toc14464799)

[2.1.2 Network Layer 10](#_Toc14464800)

[2.1.3 Application Layer 10](#_Toc14464801)

[2.2 Network Communication Protocols 10](#_Toc14464802)

[2.2.1 Bluetooth 10](#_Toc14464803)

[2.2.2 Wi-Fi 11](#_Toc14464804)

[2.2.3 ZigBee 11](#_Toc14464805)

[2.2.4 HART 11](#_Toc14464806)

[2.3 Application Communication Protocols 12](#_Toc14464807)

[2.3.1 Message Queue Telemetry Transport 12](#_Toc14464808)

[2.3.2 Advanced Message Queueing Protocol 13](#_Toc14464809)

[2.3.3 Constrained Application Protocol 14](#_Toc14464810)

[2.3.4 REdis Serialization Protocol 15](#_Toc14464811)

[2.4 Data Exchange Formats 16](#_Toc14464812)

[2.4.1 XML 16](#_Toc14464813)

[2.4.2 JSON 16](#_Toc14464814)

[2.4.3 Protocol Buffers 17](#_Toc14464815)

[2.5 Security Threats 18](#_Toc14464816)

[2.5.1 DOS Attack 18](#_Toc14464817)

[2.5.2 Man in The Middle Attack 19](#_Toc14464818)

[2.5.3 Malicious Code Attack 20](#_Toc14464819)

[2.5.4 Physical Tampering 20](#_Toc14464820)

[2.5.5 Botnet 20](#_Toc14464821)

[2.5.6 Brute Force Attacks 20](#_Toc14464822)

[2.6 Security Guidelines for Internet of Things 21](#_Toc14464823)

[2.6.1 Machine-To-Machine Communication 22](#_Toc14464824)

[2.6.2 Firewall Protection 23](#_Toc14464825)

[2.6.3 Asymmetric Cryptography 23](#_Toc14464826)

[2.7.4 Symmetric Cryptography 23](#_Toc14464827)

[2.7 Password Handling 24](#_Toc14464828)

[2.7.1 Password Hashing 25](#_Toc14464829)

[2.7.2 Password Salt 25](#_Toc14464830)

[2.8 Facial Recognition 26](#_Toc14464831)

[2.8.1 Haar Cascade 26](#_Toc14464832)

[2.8.2 Histogram of Oriented Gradients 27](#_Toc14464833)

[2.9 Related Works 27](#_Toc14464834)

[3.0 Technology Review 28](#_Toc14464835)

[3.1 Hardware Selection 28](#_Toc14464836)

[3.2 Operating System Selection 28](#_Toc14464837)

[3.2.1 Raspberry Pi Operating System 28](#_Toc14464838)

[3.2.2 Cyber Security Operating System 28](#_Toc14464839)

[3.3 Programming Language Selection 29](#_Toc14464840)

[3.4 Library Selection 29](#_Toc14464841)

[3.4.1 Python Library Selection 29](#_Toc14464842)

[3.4.2 C# Library Selection 30](#_Toc14464843)

[3.5 Software Review 30](#_Toc14464844)

[4.0 System Requirements 31](#_Toc14464845)

[4.1 Hardware and Software Requirements 31](#_Toc14464846)

[4.2 Functional & Non Functional Requirements 32](#_Toc14464847)

[5.0 Methodology 33](#_Toc14464848)

[5.1 Software Development Methodology 33](#_Toc14464849)

[5.2 Surveillance System Development 34](#_Toc14464850)

[5.2.1 Gathering Face Dataset 34](#_Toc14464851)

[5.2.2 Encoding Face Dataset 34](#_Toc14464852)

[5.2.3 Real Time Face Recognition 34](#_Toc14464853)

[5.2.4 MQTT Communication 35](#_Toc14464854)

[5.3 Application Development 35](#_Toc14464855)

[5.3.1 Receiving Images MQTT 35](#_Toc14464856)

[5.3.2 Database Development 35](#_Toc14464857)

[5.3.3 Displaying Received Images 35](#_Toc14464858)

[5.3.4 Password Storage 35](#_Toc14464859)

[5.4 Security Implementation 36](#_Toc14464860)

[5.4.1 Raspberry Pi Specific Security 36](#_Toc14464861)

[5.5 Security Best Practices 37](#_Toc14464862)

[6.0 System Design 38](#_Toc14464863)

[6.2 Mobile Application User Interface Design 39](#_Toc14464864)

[6.2.1 Displaying Images Sent From MQTT 39](#_Toc14464865)

[6.2.2 Log in Design 40](#_Toc14464866)

[7.0 References 41](#_Toc14464867)

# Table of Figures

[Figure 1: Smart Home - revenue forecast for the segment Security worldwide\* from 2017 to 2023 (in million U.S. dollars) (source: www.statista.com) 7](#_Toc14471618)

[Figure 2: IoT 3 layered architecture in relation to a home surveillance system 10](#_Toc14471619)

[Figure 3: MQTT Architecture using a Raspberry Pi as both a Publisher and Broker 13](#_Toc14471620)

[Figure 4: Block diagram showing basic AMQP protocol process 14](#_Toc14471621)

[Figure 5: Block diagram showing a basic GET/Response between a CoAP Client & Server 15](#_Toc14471622)

[Figure 6: Code Snippet showing basic XML Schema 17](#_Toc14471623)

[Figure 7: Code snippet showing basic JSON Schema 17](#_Toc14471624)

[Figure 8: Diagram showing a DDoS attack using infected PCs (slaves) 19](#_Toc14471625)

[Figure 9: Man in The Middle Attack showing an intercepted connection from a malicious attacker 20](#_Toc14471626)

[Figure 10: Diagram detailing the SSH Protocol for Machine-To-Machine Communication (ssh.com, 2019) 23](#_Toc14471627)

[Figure 11: Diagram comparing the two most common algorithms in a brute force attack (Putri Ratna et al., 2013) 26](#_Toc14471628)

[Figure 12: Diagram showing the most commonly detect features in the Haar Cascade algorithm 27](#_Toc14471629)

[Figure 13: Raspberry Pi Model 3b 29](#_Toc14471630)

[Figure 14: Incremental Software Development Lifecycle for a Home Surveillance System 34](#_Toc14471631)

[Figure 15: Diagram showing the main flow of the system 39](#_Toc14471632)

[Figure 16: Initial User Interface Design for Viewing Images within the App 40](#_Toc14471633)

[Figure 17: Initial User Interface Design for Login & Authentication 41](#_Toc14471634)

# Table of Tables

[Table 1: Comparison table of common IoT Network Communication Protocols 14](#_Toc14464884)

[Table 2: Table highlighting features of most common IoT Application Communication Protocols 18](#_Toc14464885)

[Table 3: Serialized size in bytes (Sumaray and Makki, 2012) 20](#_Toc14464886)

[Table 4: Average serialization time in ms (Sumaray and Makki, 2012) 20](#_Toc14464887)

[Table 5: Average deserialization time in ms (Sumaray and Makki, 2012) 20](#_Toc14464888)

[Table 6: Relevant IoT best practices in relation to the project 24](#_Toc14464889)

[Table 7: Hardware Requirements for project 34](#_Toc14464890)

[Table 8: Software Requirements for project 34](#_Toc14464891)

[Table 9: Core Functional Requirements 35](#_Toc14464892)

[Table 10: Non-Functional Requirements 35](#_Toc14464893)

[Table 11: Proposed solutions for best practices 40](#_Toc14464894)

# 1.0 Introduction

## 1.1 Background

With the recent explosion of Internet of Things devices, there is a rising concern by the general public on the security of these devices. In 2015, HP published a report that highlighted that out of the ten home security systems analysed, 100% of them had security vulnerabilities such as not requiring strong passwords and only one offered two-factor authentication (HP, 2015). Concerning reports such as the aforementioned along 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), have brought these issues into the public’s attention, raising concern about the validity of the security of these 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). The industry of Smart Security expects a revenue forecast of 28 million by the end of 2023 (shown in Figure 1), further highlighting the importance of development of secure IoT devices.



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

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 becomes non-functional.

As an alternative to the current mainstream method of hosting on the cloud, a Raspberry Pi-based security system utilising local storage is proposed. The Raspberry Pi, being a small credit card sized computer, has near unlimited capabilities in home smart technology, only limited to its processing speed and memory. Building a custom made home surveillance system poses various security challenges similar to all Internet of Things devices. Strategies such as local base storage, implementation of cryptography based MQTT communication and salt hashing algorithms are proposed to deal with the various challenges present at both the application and network layer. By investigating best security practices and covering every layer of the IoT architecture, a model can be proposed to build future similar systems.

## 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).

## 1.3 Project objectives

This project aims to achieve the following objectives:

1. Identify from the available literature, state of the art guidelines for an Internet of Things-based home surveillance system. With multiple network and communication protocols being available for IoT devices, it is important to determine the most secure and standard for this type of home system.
2. Review the Internet of Things architecture to understand security and design flaws for each layer. The perception, network and application layer currently pose various security challenges for IoT and must be addressed individually.
3. Determine the most appropriate data exchange format. With there being multiple data formats available for application communication between devices, the most suitable is selected, being determined from variables such as serialization time, deserialization time and message size.
4. Ensure the security standards are in alignment with the guidelines set by IoT security foundation (IoT Security Compliance Framework, 2018). By comparing the system to the best practices standard, it can be ensured that the system meets security requirements.
5. Identify commonly security threats to Internet of Things based devices. It is important to understand the most prominent cyber-attacks carried out on these devices to prepare defence against them.
6. With devices such as the Raspberry Pi being limited by its computational power, it is important to determine the most appropriate face recognition methodology suitable for a small device such as the Raspberry Pi.

# 2.0 Literature Review

This section covers the overall Internet of Things architecture and the current security issues present in each layer. State of the art network and communication protocols are reviewed as well as security protocols to determine the most suitable protocols for the proposed system. Various security threats are reviewed in order to understand the potential attacks that can be carried out on the system. Cybersecurity methods such as cryptography and salt hashing are reviewed to determine their suitability for the project. Finally, facial recognitions algorithms are reviewed with the computation limitations of the Raspberry Pi in mind.

## 2.1 Internet of Things Architecture

IoT security faces three main 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 (Burhan et al., 2018). This can be seen in Figure 2. For cloud based systems, an additional Processing layer is also considered (Aziz and Haq, 2018).

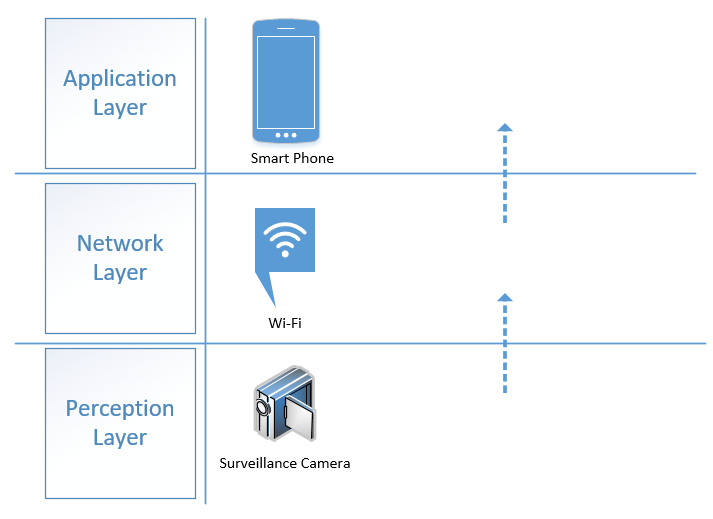


Figure : IoT 3 layered architecture in relation to a home surveillance system

### 2.1.1 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.

### 2.1.2 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. Mainstream protocols such as Wi-Fi occur at this layer, as well as lightweight protocols such as MQTT and ZigBee.

### 2.1.3 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. The user interface of any application would always be present at this layer.

## 2.2 Network Communication Protocols

Internet of Things devices differ to traditional computing devices in terms of network communication, utilising additional communication technologies such as ZigBee and Bluetooth, compared to traditional computers solely relying on Wi-Fi based communication.

The network communication protocol to be used will have the following attributes:

* An adequate range to reach the Raspberry Pi carrying out the surveillance
* Commonplace in home, to increase scalability
* High levels of security capability (encryption & authentication)
* Capable of fast data transmission (50mb/s+)

### 2.2.1 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. Bluetooth has a max signal rate of 1mb/s and an average range of 10 meters (Lee, Su and Shen, 2007).

### 2.2.2 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). Wi-Fi has the added benefit of being the fastest of all common communication technologies with a recent report showing the average speed being 16.51Mbps (Cable, 2019). The average range of a Wi-Fi connection is around 100 meters (Lee, Su and Shen, 2007).

### 2.2.3 ZigBee

ZigBee is a communication protocol, which utilises small, low-power and cost radios. It is frequently utilised in the smart homes in conjunction with hubs such as the Amazon Echo (ZigBee Alliance, 2019). The technology is very limited in terms of signal rate with a rate of 250Kb/s (Lee, Su and Shen, 2007), making it unsuitable for video transmission. The transmission range is rated between 10 and 100 meters. In the paper (Romashchenko, Brutscheck and Chmielewski, 2018), a secure surveillance system was created based on ZigBee and AES encryption, showing success against brute force attacks.

### 2.2.4 HART

Highway Addressable Remote Transducer or Hart for short is a communication protocol used primarily in an industrial setting due to its ability to accurately encode and decode communication signals in settings with noisy or harsh environments (Treacy, 2019). It Is considered the global standards for digital communication across analog wires between smart devices and monitoring/control systems (Instrumentation and Control Engineering, 2018).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Requirement | Bluetooth | Wi-Fi | ZigBee | Hart |
| High range |  |  |  |  |
| Commonplace in home |  |  |  |  |
| Security |  |  |  |  |
| Fast Data Transmission |  |  |  |  |

Table : Comparison table of common IoT Network Communication Protocols

As shown in the comparative table above, Wi-Fi, being the most commonly used form of network communication, is most suitable for the experiment. Being commonplace in homes along with its high range and fast data transmission feed, gives Wi-Fi a severe advantage over its networking counterparts.

## 2.3 Application Communication Protocols

### 2.3.1 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. It is based on the client/server architecture, the server being responsible for handling the clients request of receiving or sending data between each other. This means when a device sends data to the broker (client) it is ‘publishing’ data for any ‘subscribers’ listening to that particular topic.

It supports three levels of Quality of Service (QoS), with each having different volumes of packets exchanged. QoS Level 0 sends a message once and does not check if the message arrived to its given destination. Level 1 improves upon this by sending the message at least once and checks the delivery status using PUBACK, a status check message. If the PUBACK is lost, this can result in the same message being sent twice, due to no confirmation of the original message. Finally, Level 2 sends the message exactly once by utilising a 4-way handshake between the client and broker. This has the benefit of there being no possibility of the message being lost, but can cause additional delays. In a correlation analysis measuring lost and delay of MQTT QoS levels, it was found that for Levels 0 and 1, the average packet loss was around 0.90% to 1.40% whereas packet loss only occurred at maximum, 0.18% with QoS level 2 (Lee et al., 2013). Although QoS level 2 did have the highest end-to-end delay, this was at maximum one second, suggesting QoS Level 2 would be most suitable for the proposed system. Sharing the same attributes as MQTT, SMQTT introduces an encryption/decryption protocol to enhance security (Singh et al., 2015).

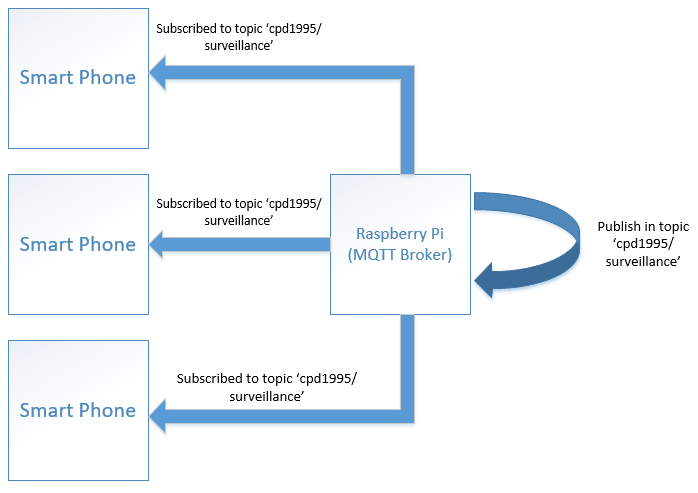


Figure : MQTT Architecture using a Raspberry Pi as both a Publisher and Broker

### 2.3.2 Advanced 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 request/response and publisher subscriber models are available with this protocol. Communication via this protocol is done through either the publisher or consumer creating an “exchange” with a given name, that name can then be broadcasted for both publishers and consumers to discover each other. Along with this exchange, the consumer creates a “queue”, attaching it to the exchange. Messages that are received by the exchange are matched to the queue via a binding process. AMQP offers the most flexibility when it comes to message exchange, offering multiple methods such as message by topic (similar to MQTT), directly, based on headers or in a fan-out form. In terms of Quality of Service, AMQP offers two types of delivery of messages: Unsettle Format and Settle Format, being similar to MQTT’s Level 0 and 1.

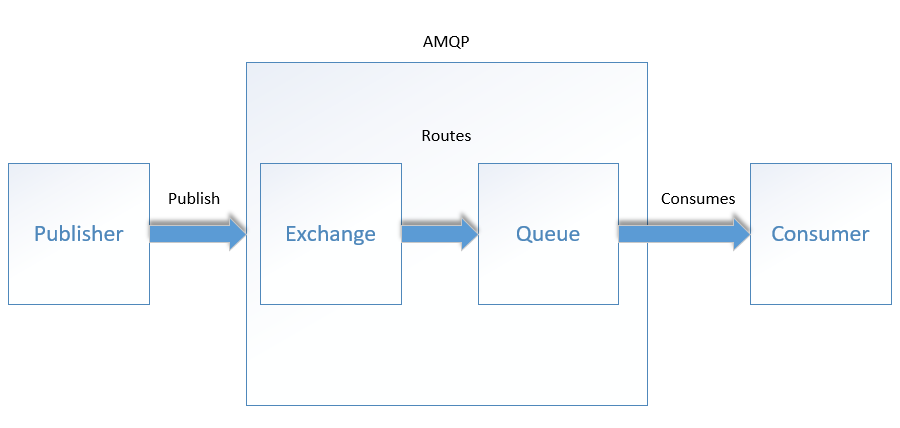


Figure : Block diagram showing basic AMQP protocol process

### 2.3.3 Constrained Application Protocol

CoAP is a stateless client/server application protocol based on the REST framework. This is based on a request/response model using the request types ‘GET’, ‘POST’, ‘PUT’ and ‘DELETE’, being similar to the standard HTTP protocol. CoAP uses Universal Resource Identifier (URI) instead of topics seen in protocols such as MQTT. This works using a similar publish/subscribe method. The publisher sends new data to the URI, and all the subscribers are notified about the new value indicated by the URI, similar to MQTT. CoAP utilises UDP as a transport protocol and DTLS for security (Ludovici, Moreno and Calveras, 2013). Using UDP instead of TCP does create less reliability as there is no guaranteed delivery of a packet. To combat this; there is the option of “confirmable” and “non-confirmable” messages to provide a Quality of Service architecture. Confirmable messages work by being acknowledged by the receiver via an ACK packet. Non-confirmable messages have no such system in place.

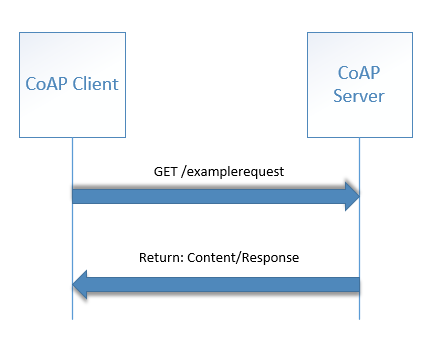


Figure : Block diagram showing a basic GET/Response between a CoAP Client & Server

### 2.3.4 REdis Serialization Protocol

RESP is an application protocol designed specifically for the Redis key-value database (Redis.io, n.d.). The main feature of this protocol is its ability to serialize data types including strings, integers and arrays. Similar to MQTT & AMQP, it is primarily used with a TCP connection. A request/response model is also used and functions by sending commands to the server. This command is then received and once processed, a response is sent back to the client. RESP has a unique feature in which responses can be scheduled; a client can send multiple commands at once and wait for a response at a later time. Another area where this protocol differs is when a client subscribes to a public/subscribe channel, it becomes a push protocol, in which the client will automatically receive messages without having to send commands.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Feature | MQTT | CoAP | AMQP | RESP |
| Header Size | 2 Byte | 4 Byte | 8 Byte | N/A |
| Architecture | Client/Broker | Client/Server or Client/Broker | Client/Server or Client/Broker | Client/Server |
| Abstraction | Publish/Subscribe | Request/Response or Publish/Subscribe | Request/Response or Publish/Subscribe | Request/Response |
| Message Size | 256mb Max | Small & Undefined | Negotiable & Undefined |  |
| QoS / Reliability | QoS 0 – At most once  QoS 1 – At least once,  QoS 2 – Exactly once | Confirmable or Non-Confirmable Message | Settle Format or Unsettle Format | N/A |
| Transport Protocol | TCP | UDP | TCP, SCTP | TCP |
| Default Port | 1883/8883 (TSL/SSL) | 5683 (UDP) | 5671/5672 (TLS/SSL) | 6379 |

Table : Table highlighting features of most common IoT Application Communication Protocols

As shown in table 2, MQTT seems to offer the most in terms of reliability of message delivery. Utilising QoS Level 2 has the guarantee the message is not lost, whereas the other protocols offer no such service, with CoAP and AMQP only offering the equivalent to a Level 1 QoS service. Transport protocol is also a consideration when selecting a communication protocol, as TCP is much more reliable than its UDP counterpart. It was also shown when it comes to sending small bytes of data similar to the payloads of most IoT devices, MQTT appears to perform better with overall less latency compared to its AMQP counterpart (Sreeraj and Kumar, 2018). In contrast, a recent comparison study found that out of all the common IoT communication protocols, MQTT was scored on the lowest in terms of security (Naik, 2017). This suggests that that SMQTT is the preferred choice for a home security system, as this protocol would meet all the given requirements.

## 2.4 Data Exchange Formats

Due to the Internet of Things still being in its infancy, there is little standardisation in most of its areas. This holds true for data exchange (Al-Fuqaha et al., 2015), with there being multiple data formats currently being used. This section aims to review the current data exchange formats and suggest the most suitable format for the proposed system.

Data serialization is the process of writing the state of an object to a stream and rebuilding this object when received on the other end. This is a way of sending and receiving data over a network. When choosing an appropriate data exchange format, the following must be considered:

* Message Size
* Serialization Time
* Deserialization Time

### 2.4.1 XML

XML, published in 1996, is one of the oldest data exchange formats created by W3C. It was designed to be used over the internet and human legible. It is text based, which can be problematic in terms of speed, as it will also need to be parsed character by character.



Figure : Code Snippet showing basic XML Schema

### 2.4.2 JSON

JSON or JavaScript Object Notation, is a message format that arose as a subset of the JavaScript programming language. It holds a similar structure to XML, being human readable with a similar schema, but with less overhead (as shown in Figure 7). In AJAX applications, JSON and XML were compared, with JSON outperforming XML in terms of data size occupancy and transmission speed (Lin et al., 2012).



Figure : Code snippet showing basic JSON Schema

### 2.4.3 Protocol Buffers

ProtoBuf is a form of protocol buffer developed by Google which utilises binary instead of text to perform fast serialization and deserialization. When compared to JSON, Protobuf outperformed JSON in both message size and speed in both Java to Java communication and Java to JavaScript, showing promising results (Krebs, 2017). The author claims Protobuf can perform up to six times faster than JSON. It should be noted that this test only tested these environments and should not be used as a whole representative for the two data exchange formats.

In a comparison study, the serialization size, average serialization time and average deserialization time were compared between XML, JSON and ProtoBuf (Sumaray and Makki, 2012). The protocol buffer outperformed both JSON and XML with XML performing the worse in every scenario (shown in Tables 3, 4 & 5). This held true regardless of the size of the object (large or small) and highlights the efficiency of the protocol buffer. Although this study was carried out on a mobile platform, it gives a clear perspective on the performance of each of the data exchange formats available for IoT communication. It can be concluded that the main advantage of using JSON is its human readable interface, which is not necessary for IoT based systems. Therefore, ProtoBuf is the most suitable due to its performance in the aforementioned qualities.

|  |  |  |  |
| --- | --- | --- | --- |
|  | XML | JSON | ProtoBuf |
| Book | 873 | 781 | 687 |
| Video | 231 | 139 | 59 |

Table : Serialized size in bytes (Sumaray and Makki, 2012)

|  |  |  |  |
| --- | --- | --- | --- |
|  | XML | JSON | ProtoBuf |
| Book | 22.284 | 4.177 | 2.339 |
| Video | 17.884 | 4.097 | 1.800 |

Table : Average serialization time in ms (Sumaray and Makki, 2012)

|  |  |  |  |
| --- | --- | --- | --- |
|  | XML | JSON | ProtoBuf |
| Book | 7.908 | 1.199 | 0.298 |
| Video | 6.742 | 0.755 | 0.197 |

Table : Average deserialization time in ms (Sumaray and Makki, 2012)

## 2.5 Security Threats

This section highlights potential security threats relating to IoT devices. The aim of this section is to uncover the most frequent security vulnerabilities present within the IoT architecture. A recent 2018 paper highlighted Denial of Service, Man in the Middle and Address Resolution Protocol poisoning being the main cyber threats to the Internet of Things (Gao et al., 2018).

### 2.5.1 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). Direct Denial of Service (DDoS) is a more extreme version of the regular DoS, which uses multiple compromised systems instead of a single unit. This is shown in Figure 8.

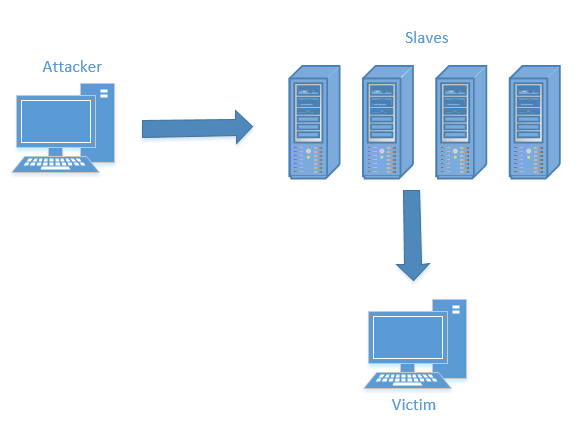


Figure : Diagram showing a DDoS attack using infected PCs (slaves)

### 2.5.2 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). ARP is a form of MITM attack that uses TCP/IP protocol used to acquire physical addresses (MAC) based on the IP addresses of nodes within the network (Abad and Bonilla, 2007). This is done through broadcasting an ARP request on the network, requesting access to the hosts IP address. When this malicious node is on the network, the node being attacked matches its physical address with the IP address of the original communication node. This is done through sending a fraudulent message to the node attacked and recording the error pairing in an APR cache table. The victim node will then communicate with the attacker node by misinterpreting the node as normal communication, sending all data (packets) towards the malicious node.

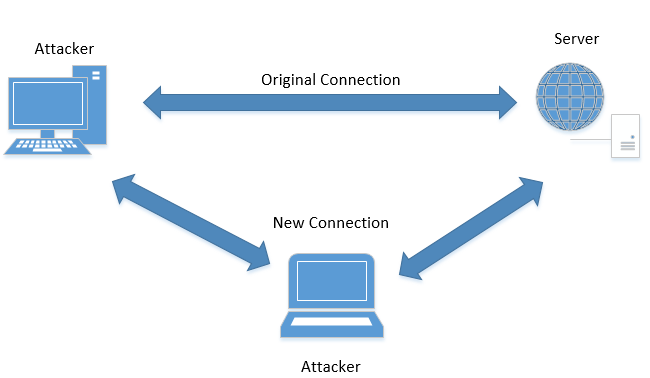


Figure : Man in The Middle Attack showing an intercepted connection from a malicious attacker

### 2.5.3 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.

### 2.5.4 Physical Tampering

Physical manipulation of a device could occur. This is when the device is modified to act in unexpected ways by someone with malicious intent. It is safe to assume that if this happens the intruder is already in the individual’s home and there is not much that can be done. A way to protect the user’s data if this occurred would be full encryption of the storage and 2-factor authentication to prevent users from accessing the micro SD that is present in the device.

### 2.5.5 Botnet

A botnet is a collection of computers performing repetitive tasks to keep websites going (Uk.norton.com, n.d.). The problem arises when this architecture is used for malicious intent, harvesting a machines power to be used in assisting in DDoS attacks. Although traditionally used against computers, IoT devices are starting to be the main target, due to their lack of security. In 2017, it was that the ‘Rakos’ botnet consisted of nearly half its entire collection being Raspberry Pi models. In 2017, it was discovered that there were various botnets designed specifically to infect IoT devices (Krebs, 2017), namely ‘Mirai’, ‘Reaper’ and ‘IoTroop’, further adding to the problem.

### 2.5.6 Brute Force Attacks

Brute force attacks consist of using software to guess as many passwords as possible while attempting to login into a system until the correct password is guessed. This could occur at device level (attempting to login to the device remotely) and at network level e.g. guessing the passphrase of a Wi-Fi router. WAP2, being the most common form of security for personal Wi-Fi routers, is susceptible to these attacks. A recent paper concluded that this protocol is especially vulnerable to dictionary based attacks and key reinstallation attacks (Abo-Soliman and Azer, 2017), which are forms of brute force attacks.

## 2.6 Security Guidelines for Internet of Things

This section highlights recommended security measures for Internet of Things-based development. In accordance with the best practices outlined by the IoT security foundation (IoT Security Compliance Framework, 2018), the following security measures have been highlighted relating to the project:

|  |  |  |
| --- | --- | --- |
| *Req. No* | *Requirement* | *Section* |
| 2.4.5.1 | Device has measures to prevent unauthenticated software and files being loaded onto it. | Software |
| 2.4.5.2 | Regarding remote software updates, software images are digitally signed and approved by the appropriate signing authority. | Software |
| 2.4.5.5 | Device disables any virtual ports not required for normal operation, the ports are disabled or only allowed to communicate with authenticated devices | Software |
| 2.4.5.6 | Watchdog timer is present and cannot be disabled to prevent stalling or disruption of operations | Software |
| 2.4.5.8 | Devices protects against unauthorised reversion of software to earlier & potentially insecure version | Software |
| 2.4.5.21 | Devices communicates over TCP, device software uses cryptography to protect data | Software |
| 2.4.6.1 | OS is implemented with relevant security updates prior to release | Process |
| 2.4.6.3 | All unnecessary logins or accounts are disabled at end of software development lifecycle | Software |
| 2.4.6.4 | Minimum access privileges required to function are assigned to relevant files, directories and data | Software |
| 2.4.6.5 | If passwords are stored on device, password files are only accessible by most privileged accounts | Software |
| 2.4.6.6 | All non-essential services have been removed from devices software | Software |
| 2.4.6.7 | All OS command line access to most privileged accounts have been removed from OS | Software |
| 2.4.6.8 | Devices OS Kernel cannot be called by external product level interfaces or unauthorised products | Software |
| 2.4.6.9 | Applications are operated at lowest privilege level and only have access to necessary resources | Software |
| 2.4.6.10 | All supported security features available on OS are enabled | Software |
| 2.4.6.11 | OS is separate from application & is only accessible via defined secure interfaces | Software |
| 2.4.7.1 | Devices prevents unauthorised connections to it, i.e. firewall enabled & internet layer protocol | Software |
| 2.4.7.4 | Device only supports versions of application layer protocols with no known vulnerabilities | Process |
| 2.4.7.5 | If unauthorised change is detected, device should alert admin | Software |
| 2.4.7.6 | All unused ports are closed & only required ports are active | Process |
| 2.4.7.10 | For any Wi-Fi connection using WPA2, secure encryption is used and WPA is disabled | Software |
| 2.4.7.13 | When a TCP protocol such as MQTT is used, it is protected by a TLS connection | Software |
| 2.4.7.18 | Device only enables network, application protocols and network services appropriate for device | Policy |
|  |  |  |
| 2.4.8.4 | Device does not accept null or blank passwords | Software |
| 2.4.8.5 | Device does not allow new passwords containing the users username | Software |
| 2.4.8.6 | Passwords entry follows industry standard | Software |
| 2.4.8.7 | Device has defence against brute force attacks | Software |
| 2.4.8.8 | Device securely stores passwords using industry standard cryptography | Software |
| 2.4.8.11 | Product only allows controlled user account access, no guest user accounts are supported | Software |

Table : Relevant IoT best practices in relation to the project

### 2.6.1 Machine-To-Machine Communication

Often when it comes to small board computers, they are difficult to access physically. In terms of the proposed system, the small device used as a surveillance system will be difficult to access without remote capabilities. A solution to this is the Secure Shell protocol or SSH as its commonly referred to. It is a method to remotely access one computing from another securely (Ylonen, 1996). Based on client-server model, a connection is established by the SSH client by connecting to the SSH server (see Figure 10). The client then uses public key cryptography to verify the identity of the SSH server. For data exchange, the protocol uses symmetric encryption and hashing algorithms, ensuring the privacy and integrity of the data sent between the two devices. Although SSH will be utilised very frequently during development, it is not necessary to have after development, as the whole system is automated. Therefore, it is recommended to disable SSH and close its associated port to help in the preventing of unauthorised access.

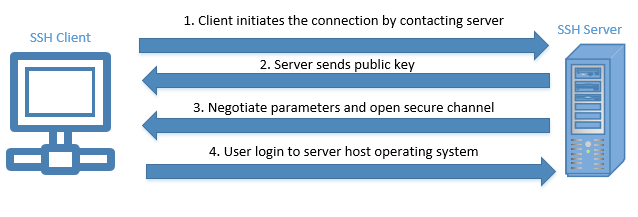


Figure : Diagram detailing the SSH Protocol for Machine-To-Machine Communication (ssh.com, 2019)

### 2.6.2 Firewall Protection

A firewall is used to enforce a set of rules regarding packet transfer and network communication. Having the ability to block suspicious traffic in an essential countermeasure against network related attacks such as Denial of Service (see 2.5.1). A recent 2018 paper highlights a rule based approach (firewall) showing successful mitigation of multiple forms of DDoS attacks against a Raspberry Pi model, suggesting this approach being highly effective (Patel and Upadhyay, 2018).

### 2.6.3 Asymmetric Cryptography

RSA works on a public-private key basis that is a form of asymmetric encryption. The public key is available to everyone, i.e. placed on the server (Raspberry Pi) whereas the private key is used to ‘unlock’ that specific public key. This gives an added layer of security as the data can only be decrypted using the individual’s private key. The private key is usually stored on a client device e.g. computer or mobile phone (Goshwe, 2013). This form of encryption was used successfully in the creation of a payment terminal using a Raspberry Pi, TSL and AES based encryption, highlighting its efficiency (Kakar, 2016). This can be used in conjunction with SSH to allow remote access to only those users that have the private key in relation to the public key, aiding in the prevention of brute force attacks.

### 2.6.4 Symmetric Cryptography

Advance Encryption Standard is symmetric form of encryption, supporting key lengths of 127, 192 and 256 bits. In a comparison study against four different algorithms, it was shown that AES has the highest avalanche effect, which is recorded as how much change there is in an output based on the change of an input. Scoring high in the avalanche effect reflects a high level of cryptographic strength. This suggests when confidentially and integrity are the highest priority, AES should be used (Patil et al., 2016).

## 2.7 Password Handling

This section highlights the importance of password handling best practices by both the user of the application and the owner. With there being various different methods of retrieving an individual’s password such as keylogging, insecure password storage and brute-force attacks, this section aims to establish the correct methodology in dealing with those threats. The UK government has provided a manual for password handling to establish best practices (ukgov, 2015):

1. Change all default passwords. When it comes to small devices like the Raspberry Pi the default username is always ‘pi’ with the password being ‘raspberry’. These should both be changed, as an unauthorised user using a remote connection such as SSH will have to guess the username as well.
2. Prioritise administrator and remote user accounts. Good practices involve not using administrator accounts for day-to-day activities with a separate account being established for this purpose. If remote access to the Raspberry Pi were granted, limits should be set on the account along with two-factor authentication to verify who is accessing the device remotely.
3. Implement a form of account lockout. As mentioned previously, brute force attacks are a large security threat to IoT devices (see 2.5.6). The UK government recommends a maximum of 10 login attempts before locking out the account.
4. Do not store passwords as plain text. If a password was stored within a database in plain text, that database being compromised leaves the users vulnerable to their details being stolen. It is recommended that passwords be stored in a form of hashing and salt combination.

### 2.7.1 Password Hashing

Password hashing is a form of one-way cryptography where text is transformed into a hash algorithm and cannot be reversed. It is used for password storage due to its key feature of non-reversal resulting in not even the owners or administrators being able to see their users’ passwords. Hashing is also used in ensuring message integrity when transferring files. Common hashing algorithms include Message Digest Algorithm (MD5) and Secure Hash Algorithm (SHA-1). In a comparative study, it was shown that regardless of password length, the SHA-1 algorithm took longer to crack, suggesting this is the superior option when it comes to password hashing (Putri Ratna et al., 2013). The results of the comparison of the two algorithms attack time against a brute force attack for a 6 character password can be seen in figure 11.



Figure : Diagram comparing the two most common algorithms in a brute force attack (Putri Ratna et al., 2013)

### 2.7.2 Password Salt

As recommended by the UK government, password hashing alone is not enough. In 2015, a paper demonstrated that regardless of hashing algorithm used, passwords were still susceptible brute-force, dictionary and rainbow-table attacks (Tatli, 2015), suggesting that without the addition of salt, passwords are not safe in a regardless hashing protocol. A salt is a random value that is considered cryptographically-string while being fixed length (Arias, 2018). This salt can be added to a hash function, which makes hash functions unique for every input, meaning if two users have the same password, the hash values for each of their passwords would not be the same, as found with traditional solo hashing. This suggests that when hashing passwords, a salt should be always added to give an additional layer of security.

## 2.8 Facial Recognition

This section covers the numerous options of face recognition algorithms. As face recognition in generally is computationally expensive, limits are imposed in terms of computational power as the Raspberry Pi’s processing power is limited.

### 2.8.1 Haar Cascade

The Haar Cascade method is a form of object detection algorithm primarily used in face detection. The purpose of the algorithm is to identify objects within a video or image based on feature selection. The algorithm is trained via positive and negative images and once trained, is then used to detect objects in other images. Each image is broken up into ‘Haar-Features’ which can be used to detect specific features of an image, the most common being edge, line and four rectangle features, the latter being used to detect slanted lines (as seen in Figure 12). Each calculated feature results in a single value by summing both rectangles and subtracting the sum of the white rectangle from the sum of the black rectangle. Although possible to calculate every single feature, there is very computationally expensive (Docs.opencv.org, n.d.).

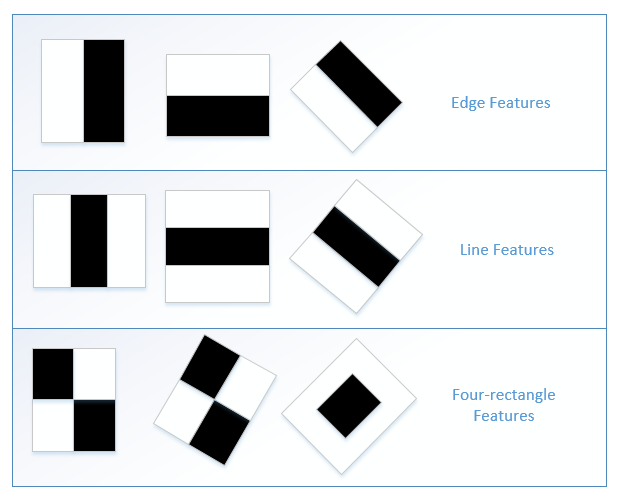


Figure : Diagram showing the most commonly detect features in the Haar Cascade algorithm

To remedy this, Adaboost is normally implemented. When it comes to training, every feature is applied on every training image. Adaboost then finds the best threshold for each feature, determining which features contain the minimum error rate. This is done through classification and is continually readjusted until the desired error rate is achieved. The resulting final classifier is a weighted sum of these weak classifiers. The term ‘weak’ is used because these features detected cannot classify an image, but when the selected features are used together, it gives strong classification results.

### 2.8.2 Histogram of Oriented Gradients

HOG is a feature descriptor used to detect objects/faces in the field of computer vision and image processing. The algorithm works by dividing the image into smaller parts via edge detection technique, being highly dependent on the orientations of the edge (Patel and Rajput, 2018). These smaller parts of the image are then further divided into small continuously connected regions called cells. There are two components of the gradient – horizontal and vertical which can be calculated using the following formula:

Magnitude of gradients =

Direction of gradients =

With the computational limitations of the Raspberry Pi considered, the HOG algorithm appears to be viable in terms of real time face detection. In their paper (Noman, Yousaf and Velastin, 2016), it is demonstrated that human detection in real time is possible using a simple Raspberry Pi model. Though promising, the author uses foreground estimation, focusing on the area in which humans have a high likelihood of appearing in the frame, to reduce the workload of the Pi. Other strategies such as greyscale conversion and background subtraction techniques were applied, further reducing the computational load on the Pi. It should be highlighted that the Raspberry Pi model used in the experiment was the model 1b, the original Pi model. This suggests that the aforementioned load reducing techniques may not be necessary on future versions of the Raspberry Pi, as the one proposed in this experiment.

## 2.9 Related Works

Raspberry Pi based home surveillance systems are not a new concept and have been created before. In a recent 2018 paper (Pawar and Umale, 2018), a home surveillance system was created using the Raspberry Pi utilising a PIR sensor to detect movement and sending an email once movement was detected. The issue with this model is that there is no way to detect who is at the door and no categorisation of whether the individual is a threat or not. Animals or other movement could also trigger the sensor leading to a false alert. Finally, the system uses email as a form of an alert system which is problematic as email can be accessed anywhere and offers little or no form of way of verifying an individual is who they say they are. A similar system was designed using face recognition technology or a password to enter a home (Hussein and Al Mansoori, 2017). Again an email is sent when there is an unknown individual at the door, posing the same problems as the previously mentioned paper. The proposed system hopes to address these challenges by using secure transport methods, 2-factor authentication and limiting the amount of potential security vulnerabilities to a single smart phone application.

# 3.0 Technology Review

This section details the various technologies proposed to carry out the experiment. This includes hardware selection, programming language choices, operating systems, various tools for security, software libraries and frameworks.

## 3.1 Hardware Selection

The Raspberry Pi model 3b was selected as the main piece of hardware due to its low cost, operating system malleability and camera support. With support for Linux based operating systems and increased processing power compared to previous models, the board is more than capable of running computer vision libraries for the surveillance system. Border surveillance was carried out successfully using a Raspberry Pi in a recent paper, demonstrating the boards capabilities. (Abdalla and Veeramanikandasamy, 2017).



Figure : Raspberry Pi Model 3b

## 3.2 Operating System Selection

### 3.2.1 Raspberry Pi Operating System

While there are multiple available OS systems available for the Raspberry Pi, Raspbian is currently the most recommend, having been designed specifically for the Raspberry Pi model (Raspbian.org, n.d.). Raspbian is an operating system based on the Linux distribution Debian, meaning it has all the features of a standard Linux operating system while being lightweight and designed for the Pi.

### 3.2.2 Cyber Security Operating System

Currently, the standard operating system used in cyber security and digital forensics is Kali Linux, derived from the Linux distribution Debian. The operating system contains over 300 programs and tools used in ethnical hacking, making it the gold standard for carrying out simulated attacks. In the 2016 paper (Liang et al., 2016), three different types of DoS attacks were carried out, resulting in all three being successful against a small IoT device.

## 3.3 Programming Language Selection

*Raspberry Pi Development*

Development on the Raspberry Pi has limitations in terms of programming language choice, with platform specific languages such as C# being severely limited due to having little support for non-Windows platforms. Python is a programming language which offers tremendous support in terms of Computer Vision, granting access to libraries OpenCV and Dlib. The only alternative languages that support these packages are C and C++. Due to time constraints and the authors previous experience with Python, it has been selected for the Raspberry Pi-based development of this experiment.

*Application Development*

Xamarin has been selected as a framework to develop a hybrid mobile application which will receive images and interact with the Raspberry Pi. Xamarin is based on Visual Studio and the programming language C# and works on a Model-View-ViewModel architecture which allows for clean separation of application logic from its user interface. A recent comparative study showed this specific feature was the biggest advantage over other hybrid and native application approaches (Vishal and Kushwaha, 2018). This, along with the authors previous experience with the programming language C#, makes Xamarin the most suitable choice for application development.

## 3.4 Library Selection

This section details the various libraries to be used in both the Raspberry Pi development and Xamarin smart phone application development. As both languages differ greatly, it is important to find the industry standard and more trustworthy packages for each language, as this will differ greatly between the two.

### 3.4.1 Python Library Selection

**OpenCV** is an open source library 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).

**Dlib**is another open source library containing support for deep learning and machine learning respectively. It has excellent image processing support, with support for SURF, HOG and FHOG algorithms and additional tools for frontal face detection (Dlib.net, n.d.).

**Imutils**is a support library for computer vision specialising in processing functions such as translation, rotation and resizing while holding support for both Python 2 and 3 respectively (GitHub, 2019). It will be used in conjunction with the computer vision OpenCV to assist in processing images.

**Pickle** is a Python library used for the serialization and deserialization of objects It is used to encode and save objects on a disk in a character stream format (GeeksforGeeks, n.d.). This stream contains all the information necessary to reconstruct the original object in a separate python script.

**Face\_Recogniton** is an open source Python library based on Dlib used to recognise and manipulate faces in a simplistic easy to used manner (GitHub, 2019). The library is used for quick face recognition and can be used in live video stream. Being compact and lightweight makes it ideal for a Raspberry Pi surveillance system.

### 3.4.2 C# Library Selection

**SQLite** is a lightweight version of SQL that can be used within the Xamarin platform. SQLite has the main advantage of being serverless and extremely lightweight with the library being less than 500KiB in size (Sqlite.org, n.d.). Being serverless has the advantage of being able to read and write to the database without a network protocol such as TCP/IP. This, along with its lightweight build, make it suitable for smart phone database storage.

**M2Mqtt** is a MQTT client made for all .Net platforms, including support for Internet of Things and M2M communication (GitHub, 2019). Other MQTT clients such as MQTTnet are platform specific and therefore not applicable to Xamarin development

## 3.5 Software Review

**Fail2Ban**: is a Python based open source software that interacts with the Raspberry Pi’s operating system’s firewall (Fail2ban.org, n.d.). Its main purpose is to ban IPs that show malicious intent. This includes too many password attempts, seeking for exploits, etc. It is recommended by the Raspberry Pi Foundation, giving it additional credibility (Raspberrypi.org, n.d.). The software is also claimed to help protect again DDoS attacks (George, 2019).

# 4.0 System Requirements

This section details the hardware and software requirements required to carry out the project. Functional and non-functional requirements are highlighted along with each requirement having a priority level. This is important as criteria with the highest level of priority should always be carried out first, whereas non-functional requirements are additional and should be treated as such.

## 4.1 Hardware and Software Requirements

This section refers to both the software and hardware requirements required for the project. Hardware requirements (see Table 6) are established, with each hardware requirement having an additional backup in case of malfunction. Software requirements are also listed (see Table 7) to highlight the relevant programming languages & libraries required for the competition of this project.

|  |  |  |
| --- | --- | --- |
| # | Requirement | Priority |
| 1 | Raspberry Pi Model 3b | High |
| 2 | Raspberry Pi NoIR Camera | High |
| 3 | Computer | High |

Table : Hardware Requirements for project

|  |  |  |  |
| --- | --- | --- | --- |
| # | Requirement | Justification | Priority |
| 1 | Raspbian Operating System | Optimised operating system made specifically for the Raspberry Pi model | High |
| 2 | Python Programming Language | Has industry standard face recognition libraries and MQTT support | High |
| 3 | Python Library - OpenCV | Package used for computer vision | High |
| 4 | Python Library - Face\_Recognition | Package used for face recognition modules | High |
| 5 | Python Library - Dlib | Package used for computer vision | High |
| 6 | Python Library – Imutils | Support package for computer vision | Medium |
| 7 | Python Library – Pickle | Package used for object deserialization | Medium |
| 8 | C# Library – SQLite | Package used for read/writing to an SQLite database | High |
| 9 | C# M2Mqtt | Package used for creation of MQTT client | High |
| 10 | Kali Linux | Operating system used for cybersecurity | High |

Table : Software Requirements for project

## 4.2 Functional & Non Functional Requirements

This section highlights the functional & non-functional requirements for the development of this project. Development of the functional requirements is carried out first, with those of highest priority completed before other lower priority task. Once the core system is completed, all security related requirements are prioritised with the intention of making the system as secure as possible. Table 9 highlights the core functionality of the system with Table 10 referring to the non-functional requirements.

|  |  |  |
| --- | --- | --- |
| # | Requirement | Priority |
| 1 | The system allows for photos to be taken from the camera of an individual initially to train the model on recognising their faces | High |
| 2 | The system can encode each image to allow for training to occur | High |
| 3 | The system can use the trained model to identify family members during a live video stream | High |
| 4 | The system can identify individuals that are not recognised as family members during a live video stream | High |
| 5 | The system can capture an image when a person is detected but not identified as a family member | High |
| 6 | The system can label the image with the current date time | Medium |
| 7 | The system can store images into a database | High |
| 8 | The system can securely send the image with relevant details via MQTT | High |
| 9 | All smartphone devices subscribed to the topic can receive the image | High |

Table : Core Functional Requirements

|  |  |  |
| --- | --- | --- |
| # | Requirement | Priority |
| 1 | Raspberry Pi should have no open unused ports | High |
| 2 | When SSH port is open, only devices with the RSA private key in relation to the Raspberry Pi RSA public key | High |
| 3 | Both default username and password of the Raspberry Pi are changed, password requirements are in alignment with described in 2.6.3 | High |
| 4 | Access privileges are limited to accounts with SSH access | High |
| 5 | MQTT communication is done securely using Secure MQTT outlined in 2.3.1 | High |
| 6 | Raspberry Pi is encrypted at operating system level | Medium |
| 7 | Database storing image files is encrypted | High |
| 8 | Smartphone users have 2-factor authentication for verification | High |
| 9 | System has protection in place to deal with security threats outlined 2.5 | High |
| 10 | System periodically deletes images on all mobile devices within the smart phone app | Medium |
| 11 | UI of smartphone app is aesthetically pleasing | Low |

Table : Non-Functional Requirements

# 5.0 Methodology

## 5.1 Software Development Methodology

With there being three main areas of criteria with the outlined functional and non-functional requirements, an Incremental Development Lifecycle is proposed. With an incremental approach, each part of the product goes through a design, implementation and testing stage, known as a ‘build’. This project naturally falls into three parts, being Raspberry Pi (surveillance system) requirements, application development requirements and security specific non-functional requirements. With this approach, each area of the project can be handled separately and ensured that the system is fully functional before attempting to implement security practices. The following build stages is proposed:

1. Surveillance system development. This includes everything relating to the Raspberry Pi such as face recognition, model training, capturing and encoding images, database storage etc.
2. Application related development. Development of a smart phone app used to communicate with the system remotely and to receive images of possible intruders at the door. This includes the implementation of the application communication protocol MQTT.
3. Security related development. After the foundational functional requirements are met, security is incorporated into all three layers of the Internet of Things architecture (see 2.1), with the requirements with the highest priority being accomplished first.

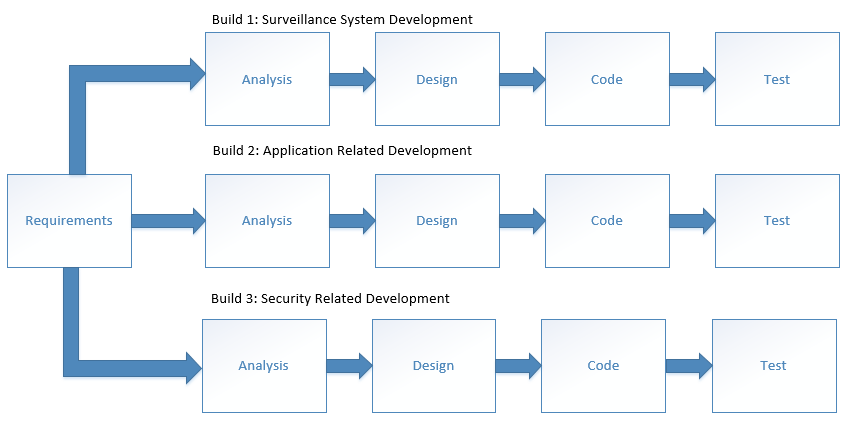


Figure : Incremental Software Development Lifecycle for a Home Surveillance System

## 5.2 Surveillance System Development

This section details the steps of development relating to the Raspberry Pi development of the incremental lifecycle. The section is further broken down into smaller components relating to creating a recognisable face dataset and constructing it into a machine readable format, carrying out the face recognition in real time and finally sending the image using MQTT as a mode of transport.

### 5.2.1 Gathering Face Dataset

As mentioned in the Literature Review, face recognition algorithms need to be trained with data (images) in order to recognise an individual’s face. With there being multiple different ways of retrieving images such as using family photos or images already taken, a solution of using the Pi camera has been proposed. The former recommended way of retrieving images can be problematic as there could be multiple people within the photos and the individual must be facing the camera directly to train the frontal view. Using the Raspberry Pi camera, a script is run with can capture images when pressing the Q image, allowing for as many images to be taken as need be.

### 5.2.2 Encoding Face Dataset

For the face images to be read and recognised by a face recognition algorithm, serialization must occur. Serialization is done via the Pickle class which serialises an object before writing it to a file. To reduce strain on the computer processing unit (CPU), the Face\_Recognition class is utilised before encoding the image files. This library can easily detect the face within the image before writing the encoding, meaning only the actual face of the individual will be encoded rather than the full image. As this is a one-time process and not done in real time, a Convolutional Neural Network approach is used. This, being a form of deep learning, is the most computationally expensive approach to face recognition, though most accurate as shown in Section 2.7.

### 5.2.3 Real Time Face Recognition

As discussed previously, Deep Learning approaches are very computationally expensive and function best running on graphics card instead of a central processing unit (CPU). This suggests this form of face recognition is not suitable for being ran on a Raspberry Pi board in real time, suggesting a different approach is to be taken. Histogram of Oriented Gradients, while shown as less accurate, is still more than capable for the objective of this paper. The theoretical of compiling the recognised faces using a Convolutional Neural Network approach and then comparing them in real time using the HOG approach could net greater accuracy without the compromise of computational expensiveness.

### 5.2.4 MQTT Communication

As discussed in Section 2.2, MQTT has been determined as the most suitable and reliable approach to communication between the app and the Raspberry Pi. Once an unrecognised face appears on the video stream, an image could be captured, and a separate script could be executed used for sending the file via MQTT. In terms of image formatting, JPG is the most suitable. Small sacrifices in image quality compared to its PNG format counterpart are a suitable trade-off for its significantly smaller size. All smart phone apps connected to the topic, could then receive the image and be notified via push notification.

## 5.3 Application Development

As concluded in the Technology Review section, a hybrid application development approach is taken due to ease of developments and time constraints on the project.

### 5.3.1 Receiving Images MQTT

The fundamental and most important part of the application development is its ability to communicate with the Raspberry Pi. Once an image is sent via MQTT, the image must be able to reconstructed in a format supported by Xamarin.

### 5.3.2 Database Development

For the images to be stored and viewed by the user, SQLite has been proposed to store the image data along with the timestamp of when it was received. The image, encoded in Base64, can be stored in that format and reconstructed when requested by the user. Additionally, to grant access to the app, the user must login, therefore an additional database must be created to store the usernames and password of each family member.

### 5.3.3 Displaying Received Images

Push notification permissions must be enabled in both iOS and Android for the user to be notified when an image is sent through MQTT. This push notification will notify the user of someone being at his or her door and once pressed will show the image of the potential intruder on screen.

### 5.3.4 Password Storage

To access the images and application, a username and password must be supplied. This is the initial layer of authentication and security to verify the individual is who they say they are. As outlined in Section 2.7, password hashing along with a salt will be used to ensure that the passwords are safe in the case of a dictionary or brute force attempt by a malicious individual.

## 5.4 Security Implementation

The final step of the incremental lifecycle is securing the project using the various methods discussed in Section 2.6. With the core functionality finished, each individual component and layer of the project must secured in accordance with the standards outlined by the Internet of Things Security Foundation.

### 5.4.1 Raspberry Pi Specific Security

This section details security measures specific to the Raspberry Pi 3b board along with its predominately-used operating system, Raspbian. According to the Raspberry Pi official documentation, the following are considered best practices (Raspberrypi.org, n.d.) for securing the device:

1. Change both the default username and password. Protocols such as SSH require both a username and password to access a remote device. The default username and password for the Raspberry Pi is ‘pi’ and ‘raspberry’ for all devices. By changing these we add another layer of security by limiting the amount of information an individual with malicious intent has.
2. Sudo command should require a password. Sudo in Linux operating systems allows commands to be run with admin privileges. By doing this a user must know the password required in order to execute commands at a higher level.
3. Ensure latest security fixes. This means having the most recent up-to-date version of the operating system and ensuring SSH is up to date.
4. Use key-based authentication. As discussed in the Cryptography section there are various ways of encrypting a service. By forcing an encryption based authentication, an additional layer of security is added as now there are two factors required to login.
5. Firewall installation. By default, the firewall available on the Raspbian operating system is not configured and must be setup by the user.

# 6.0 System Design

The main functionality of the system is based on two common scenarios, one being an identified (family or friend) enters the premises and no alert is send to the family members. Another is if the person is unidentified, then an image is captured and sent via MQTT to each the users containing the application (See Figure 15).

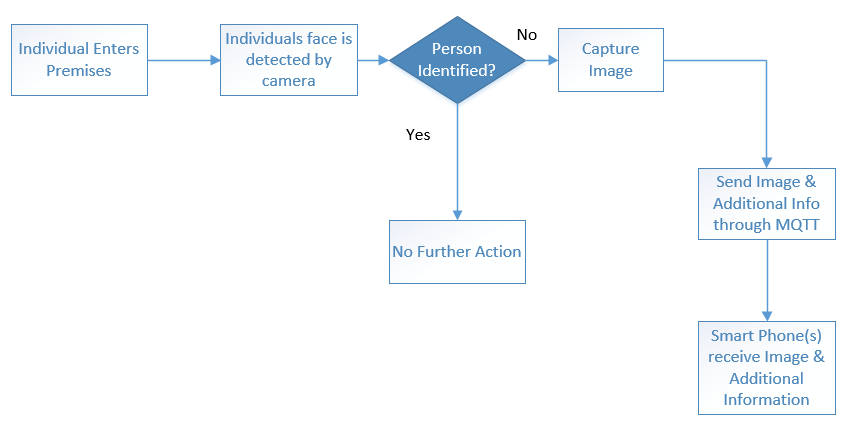


Figure : Diagram showing the main flow of the system

## 6.1 Mobile Application User Interface Design

This section details the initial screen designs for the mobile application. As development is carried out using Xamarin, the user interface stays consistent with both versions of the app. The only minor changes would be the addition on an on screen back button for when viewing images on iOS dues to its absence of a physical back button.

### 6.1.1 Displaying Images Sent from MQTT

As displaying the images sent from the Raspberry Pi model is the core functionality of the application, this is highly prioritised in terms of user interface design. For security purposes, the images within the application can only be shown while the user is logged in. The user can then view all recent images within a list view and select an image to allow for viewing the image on a larger scale. The option to delete the image is also available on this screen (see Figure 16).



Figure : Initial User Interface Design for Viewing Images within the App

### 6.2.2 Log in Design

For the user to access images and options on the control panel, they must be logged in. This is carried out by entering their username and password. To ensure authentication, touch ID will be implemented as a form of two-factor authentication. This will also to use to access the app when the user opens it after a set period of time, regardless of if the user is logged in or not.

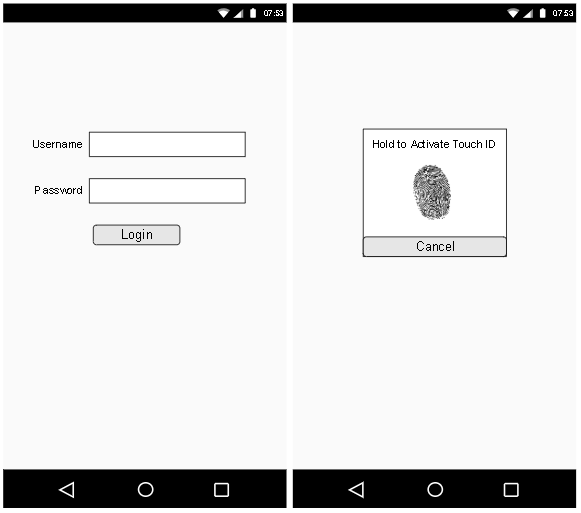


Figure : Initial User Interface Design for Login & Authentication

# 7.0 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. 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].
13. 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].
14. 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].
15. Ssh.com. (2019). *SSH Protocol – Secure Remote Login and File Transfer | SSH.COM*. [online] Available at: https://www.ssh.com/ssh/protocol/#sec-How-to-Cite-SSH [Accessed 13 Jun. 2019].
16. Ylonen, T. (1996). SSH - Secure Login Connections over the Internet. *Proceedings of the 6th USENIX Security Symposium*, pp.37-42.
17. Abo-Soliman, M. and Azer, M. (2017). A study in WPA2 enterprise recent attacks. *2017 13th International Computer Engineering Conference (ICENCO)*. [online] Available at: https://ieeexplore.ieee.org/document/8289808 [Accessed 13 Jun. 2019].
18. Sreeraj, S. and Kumar, G. (2018). Performance of IoT protocols under constrained network, a Use Case based approach. *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*. [online] Available at: https://ieeexplore.ieee.org/document/8668105 [Accessed 13 Jun. 2019].
19. Singh, M., Rajan, M., Shivraj, V. and Balamuralidhar, P. (2015). Secure MQTT for Internet of Things (IoT). *2015 Fifth International Conference on Communication Systems and Network Technologies*. [online] Available at: https://ieeexplore.ieee.org/abstract/document/7280018 [Accessed 13 Jun. 2019].
20. How safe are home security systems? (2015). [ebook] HP. Available at: http://go.saas.hpe.com/l/28912/2015-07-21/32bhy5/28912/69170/IoT\_Home\_Security\_Systems.pdf [Accessed 13 Jun. 2019].
21. Goshwe, N. (2013). Data Encryption and Decryption Using RSA Algorithmin a Network Environment. *IJCSNS International Journal of Computer Science and Network Security*, [online] VOL. 13(No. 7). Available at: http://paper.ijcsns.org/07\_book/201307/20130702.pdf [Accessed 16 Jun. 2019].
22. Kakar, V. (2016). Secure communication and authentication using Raspberry Pi. *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. [online] Available at: https://ieeexplore.ieee.org/document/7785011 [Accessed 16 Jun. 2019].
23. Patil, P., Narayankar, P., Narayan D.G. and Meena S.M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, [online] 78, pp.617-624. Available at: https://www.sciencedirect.com/science/article/pii/S1877050916001101?via%3Dihub [Accessed 16 Jun. 2019].
24. Lee, S., Kim, H., Hong, D. and Ju, H. (2013). Correlation analysis of MQTT loss and delay according to QoS level. *The International Conference on Information Networking 2013 (ICOIN)*. [online] Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7428475 [Accessed 17 Jun. 2019].
25. Ludovici, A., Moreno, P. and Calveras, A. (2013). TinyCoAP: A Novel Constrained Application Protocol (CoAP) Implementation for Embedding RESTful Web Services in Wireless Sensor Networks Based on TinyOS. *Journal of Sensor and Actuator Networks*, [online] 2(2), pp.288-315. Available at: https://www.researchgate.net/publication/276039057\_TinyCoAP\_A\_Novel\_Constrained\_Application\_Protocol\_CoAP\_Implementation\_for\_Embedding\_RESTful\_Web\_Services\_in\_Wireless\_Sensor\_Networks\_Based\_on\_TinyOS [Accessed 17 Jun. 2019].
26. Naik, N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. *2017 IEEE International Systems Engineering Symposium (ISSE)*. [online] Available at: https://ieeexplore.ieee.org/document/8088251 [Accessed 17 Jun. 2019].
27. UK Government advice on Password Guidance, Simplifying your approach. (2015). [ebook] CESG and CPNI. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/458857/Password\_guidance\_-\_simplifying\_your\_approach.pdf [Accessed 18 Jun. 2019].
28. Fail2ban.org. (n.d.). *Fail2ban*. [online] Available at: https://www.fail2ban.org/wiki/index.php/Main\_Page [Accessed 18 Jun. 2019].
29. Cable. (2019). *Worldwide Broadband Speed League 2018 | Cable.co.uk*. [online] Available at: https://www.cable.co.uk/broadband/speed/worldwide-speed-league/ [Accessed 20 Jun. 2019].
30. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, [online] 17(4), pp.2347-2376. Available at: https://ieeexplore.ieee.org/document/7123563 [Accessed 20 Jun. 2019].
31. Krebs, B. (2017). *Beating JSON performance with Protobuf*. [online] Auth0 - Blog. Available at: https://auth0.com/blog/beating-json-performance-with-protobuf/ [Accessed 20 Jun. 2019].
32. Lin, B., Chen, Y., Chen, X. and Yu, Y. (2012). Comparison between JSON and XML in Applications Based on AJAX. *2012 International Conference on Computer Science and Service System*. [online] Available at: https://ieeexplore.ieee.org/document/6394535 [Accessed 20 Jun. 2019].
33. Sumaray, A. and Makki, S. (2012). A comparison of data serialization formats for optimal efficiency on a mobile platform. *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication - ICUIMC '12*. [online] Available at: https://dl.acm.org/citation.cfm?id=2184810 [Accessed 20 Jun. 2019].
34. 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].
35. Raspbian.org. (n.d.). *FrontPage - Raspbian*. [online] Available at: https://www.raspbian.org/ [Accessed 21 Jun. 2019].
36. Raspberrypi.org. (n.d.). *Securing your Raspberry Pi - Raspberry Pi Documentation*. [online] Available at: https://www.raspberrypi.org/documentation/configuration/security.md [Accessed 21 Jun. 2019].
37. George, G. (2019). *How to secure your Raspberry Pi board [Tutorial] | Packt Hub*. [online] Packt Hub. Available at: https://hub.packtpub.com/how-to-secure-your-raspberry-pi-board-tutorial/ [Accessed 21 Jun. 2019].
38. Uk.norton.com. (n.d.). *What Is A Botnet?* [online] Available at: https://uk.norton.com/internetsecurity-malware-what-is-a-botnet.html [Accessed 21 Jun. 2019].
39. Krebs, B. (2017). *Reaper: Calm Before the IoT Security Storm? — Krebs on Security*. [online] Krebsonsecurity.com. Available at: https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm/ [Accessed 21 Jun. 2019].
40. Dlib.net. (n.d.). *dlib C++ Library*. [online] Available at: http://dlib.net/ [Accessed 24 Jun. 2019].
41. Docs.opencv.org. (n.d.). *OpenCV: Face Detection using Haar Cascades*. [online] Available at: https://docs.opencv.org/3.4.1/d7/d8b/tutorial\_py\_face\_detection.html [Accessed 24 Jun. 2019].
42. Treacy, F. (2019). *HART Communication Made Easy*. [ebook] Available at: https://www.analog.com/media/en/technical-documentation/technical-articles/HART\_Communication\_Made\_Easy.pdf [Accessed 24 Jun. 2019].
43. Instrumentation and Control Engineering. (2018). *HART ( Highway Addressable Remote Transducer) Communication Protocol*. [online] Available at: https://automationforum.co/hart-highway-addressable-remote-transducer-communication-protocol/ [Accessed 24 Jun. 2019].
44. Redis.io. (n.d.). *Redis Protocol specification – Redis*. [online] Available at: https://redis.io/topics/protocol [Accessed 25 Jun. 2019].
45. Patel, K. and Upadhyay, H. (2018). *A Rule based Approach to Mitigate DDoS attack in IoT Environment*. [ebook] Available at: https://pdfs.semanticscholar.org/a8af/1a108244b37d1994962e5f250875f0adb1ab.pdf [Accessed 25 Jun. 2019].
46. Abad, C. and Bonilla, R. (2007). An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks. *27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07)*. [online] Available at: https://ieeexplore.ieee.org/document/4279062 [Accessed 28 Jun. 2019].
47. GitHub. (2019). *jrosebr1/imutils*. [online] Available at: https://github.com/jrosebr1/imutils [Accessed 28 Jun. 2019].
48. GeeksforGeeks. (n.d.). *Understanding Python Pickling with example - GeeksforGeeks*. [online] Available at: https://www.geeksforgeeks.org/understanding-python-pickling-example/ [Accessed 28 Jun. 2019].
49. GitHub. (2019). *ageitgey/face\_recognition*. [online] Available at: https://github.com/ageitgey/face\_recognition [Accessed 28 Jun. 2019].
50. 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/stamp/stamp.jsp?tp=&arnumber=8697345 [Accessed 5 Jul. 2019].
51. Hussein, N. and Al Mansoori, I. (2017). Smart Door System for Home Security Using Raspberry pi3. *2017 International Conference on Computer and Applications (ICCA)*. [online] Available at: https://ieeexplore.ieee.org/document/8079785 [Accessed 5 Jul. 2019].
52. Tatli, E. (2015). Cracking More Password Hashes with Patterns. *IEEE Transactions on Information Forensics and Security*, [online] 10(8), pp.1656-1665. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7084670 [Accessed 18 Jul. 2019].
53. Arias, D. (2018). *Adding Salt to Hashing: A Better Way to Store Passwords*. [online] Auth0 - Blog. Available at: https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/ [Accessed 18 Jul. 2019].
54. Patel, H. and Rajput, R. (2018). Smart Surveillance System Using Histogram of Oriented Gradients (HOG) Algorithm and Haar Cascade Algorithm. *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*. [online] Available at: https://ieeexplore.ieee.org/document/8697464 [Accessed 19 Jul. 2019].
55. Noman, M., Yousaf, M. and Velastin, S. (2016). An Optimized and Fast Scheme for Real-Time Human Detection Using Raspberry Pi. *2016 International Conference on Digital Image Computing: Techniques and Applications (DICTA)*. [online] Available at: https://ieeexplore.ieee.org/document/7797008 [Accessed 19 Jul. 2019].
56. Sqlite.org. (n.d.). *Distinctive Features Of SQLite*. [online] Available at: https://www.sqlite.org/different.html [Accessed 19 Jul. 2019].
57. GitHub. (2019). *eclipse/paho.mqtt.m2mqtt*. [online] Available at: https://github.com/eclipse/paho.mqtt.m2mqtt [Accessed 19 Jul. 2019].