IoT layered architecture risks and cybersecurity threats in Smart Home

Candidate number:

Technical Report
RHUL-ISG-2021
Aug. 24, 2021

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Candidate Number:

IoT layered architecture risks and cybersecurity threats in Smart Home

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London

I declare that this assignment is all my work and that I have acknowledged all quotations from published or unpublished work of other people. I also say that I have read the statement on plagiarism in Section 1 of the Regulation Governing Examination and Assessment Offences, and in according with those regulations, I submit the project report as my work.

Signature: 2110919

Date: Aug. 24, 2021

ACKNOWLEDGMENT

I would like to express my appreciation to my supervisor for his support and guidance.

TABLE OF CONTENT

List of Figures &Tables

EXECUTIVE SUMMARY

Smart Home is an emerging paradigm focusing on connecting devices.
In this way, Smart Home advocates aim to create a smart environment for its inhabitants, but here is where the fundamental question comes! How Smart is your Smart Home? This research aims to answer this question! By investigating and analysing IoT layered architecture in Smart Home and conducting a risk assessment exercise. Later, those conducted exercises have reported that there are rather too many weak points in Smart Home layered architecture that a malicious party could exploit.

Furthermore, those overall results showed that IoT layered architecture is insecure as the architecture is prone to various cybersecurity attacks. Each layer came with its own set of weaknesses that can exploit by hackers once they are known to them. To meet this study's aims and objectives, mitigation actions to each layer have been suggested.

Based on the analysed risks and cybersecurity threats of the existing four-layered architecture, it becomes clear that is an emerging need for new and more secure IoT layered architecture. An improved model of seven-layered architectures has been proposed. This model will provide better security of the system as fog and cloud layers are included in the communication. In this way, smart home devices will communicate first with fog and cloud layers before communicating with the network layer, and that will provide a better overall security of Smart Home systems. Furthermore, the cloud layer will support the normal operational function of the devices by providing a regular software update.

One of the main aims of this project was to make end-users, manufacturers and IT consultants aware of the current risks and threats of IoT layer architecture in Smart Home. This study would not be relevant to end-users if real cases were excluded. Therefore, this research has adopted three real-world cases. Each case was studied with details by describing the potential vulnerabilities, the impact of those vulnerabilities to Smart Home users and their family members and suggesting a suitable countermeasure that can be applied. By providing relevant cases, the findings and the results of those cases, this project met its aims and objectives. It reached its final goal to educate end-users about risks and threats in layered architecture vie Smart Home.

1 Introduction

Internet of Things (IoT) provides connectivity for anyone at any time and at any place. The IoT technologies are moving forward society where everything and everyone will be connected to the internet, including your home which will become so-called Smart Home.

Smart Home is a combination of various subsystems and advanced technologies that can share and communicate information within the house instantly and externally through a smart home gateway[1].

The Smart Home innovation will “offers convenience and efficiency to the home residents so that they can achieve a better quality of life” [2].On the other side Manufactures and IT Consultants will be able to transform customer experience, enrich devices functionality, improve product maintenance, and create of new business opportunities [3].

It is estimated that there are going to be around 30 billion IoT devices by 2022 [4] those IoT devices will stream data through the fifth generation (5G) network to cloud based. This IoT-generated data will help” train algorithms and allow machine–to–machine to operate seamlessly” [2], so no human intervention will be needed after all, and your home will become an automated home that will be able to operate with minimum human intervention.

However, most of the IoT devices in Smart Home will be low cost and wirelessly connected. Therefore, the IoT devices will need to be part of a secure network in a team to be able to protect the confidentiality, integrate and availability of the system.

It has been reported in several studies that IoT devices are insecure[4] and that they are facing an enormous number of cybersecurity challenges. Those challenges are related to "authentication, authorisation, information leakage, privacy, and verification".[4]

According to industry experts, in 2023, 25 percent of all cyberattacks will target IoT devices. Attacks such as viruses, worms, and botnets are easily achievable on IoT devices [5]simple because those devices are unsecure and provide easy access to the target system.

Therefore, this thesis aims to study the security issues of IoT vie Smart Home. As the technologies keep evolving, users are given the option to add additional IoT devices to their homes and create even smarter homes. From a smart kettle to a smart light and smart dog feeder and so on, the list of smart home devices that manufactures are producing today is long.

In fact, all our daily devices are becoming smart today, however as end-user keep on adding more IoT devices to their home the management of such as system become more complex and vulnerable to cyber-attacks.

1.2 Aims and Objectives.

1.2.1 Aim

This project aims to investigate the existing security vulnerabilities and threats in Smart Home devices also to provide an effective guide which will helps stockholders on how to protect those devices. To achieve this aim, the following objectives should be fulfilled.

1.2.2 Objectives

Objective 1: Identify, describe, and illustrate IoT devices in Smart Home.

Objective 2: Identify and describe the benefits and risks of IoT devices in Smart Homes.

Objective 3: Identify and describe IoT-based Smart Home architecture and how it functions?

Objective 4: Identify and describe the common four-layered IoT architecture and the types of cyber-attacks the architecture is vulnerable to?

Objective 5: Propose a suitable framework vie risk assessment of IoT devices in Smart Home.

Objective 6: Provide a suitable countermeasure for the vulnerable IoT devices in Smart Home based on the risk assessment framework.

Objective 7: Provide effective recommendations for end-users, IT consultants and manufactures on how to minimise the identified security vulnerability of IoT devices in Smart Homes.

1.3 Scope

This thesis will focus on the security consideration of Smart Home and IoT devices.

Firstly, I will identify common IoT devices used in Smart Home and look at how Smart Home functions as a system by studying the architecture of Smart Home and then I will identify and describe the benefits and risks of Smart Home.

Later, I will focus on the Smart Home technology and describe some of the most common cyber-attacks those IoT devices are vulnerable to.

Based on research, the documentation, reports, and studies that have been produced so far purely focus on IoT vulnerability in enterprise settings, and very limited studies have been conducted on IoT security in-home settings, therefore this study aims to produce a risk assessment framework that will help Smart Homeowners to protect their IoT devices from cyber-attacks and make them aware of the vulnerabilities of those IoT devices.

To support my recommendation, I will reference OCTAVE allegro methodology and justified the findings of the project by referring to some relevant case studies.

1.4 Methodology and Structure

1.4.1 Research design

The methodology of this project will follow a qualitative research design which is often "associated with interpretive philosophy. It is interpretive because the researcher needs to make sense of the subjective and socially constructed meanings expressed about the phenomenon being studied" [6]

This study aims to collect and analysis secondary data from the following sources:

- Books
- Case Studies
- The Internet
- Research Publication

1.4.2 Research Approach

This thesis aims to use a “deductive approach which involved the development of theory that been subject to rigorous test through a series of propositions. As, such a dominant research approach in the natural science, where laws present the basis of explanation, allow the anticipation of phenomena, predict their occurrence and therefore permit them to be controlled” [6].

1.4.3 Research Strategy

The research strategy of the project is intended to use multiple case studies, which will be carefully selected based on relevant content, to meet the aims and objectives of the project. [7] “proposes that multiple case study strategy may combine a small number of cases chosen to predict literal replication and a second small number chosen to predict theoretical replication. Where all the findings from those cases are as predicted, this would clearly produce very strong support for the theoretical propositions on which those predications were based“ [7], but if my findings are in some way contrary to the predictions “in the theoretical propositions being tested, it would be necessary to reframe those propositions and chose another set of cases to test them”[6] As according to [7] “case studies are in-depth- inquiry into a topic or phenomenon. Case study strategy has the capability to generate insight from intensive and indepth research, leading to rich, empirical descriptions and the development of theory” [6] However, case study research is likely to prove challenging because of its “intensive and in-depth nature and the needs to be able to identify, define and gain access to a case study setting” [6].

1.4.4 Chapter Structure

Each chapter will begin with a chapter introduction and detail the theme and the structure of the chapter.

Chapter 1 Aims to introduce the chapter to the reader by providing an overview of the IoTbased Smart Home technology and the current trends of the market.

Chapter 2 Provide a few different definitions of Smart Home and describe the advantages, disadvantages, the architecture of Smart Home. This chapter aims to investigate the security concerns and threats of Smart Home.

Chapter 3 Study a traditional four-layer architecture of IoT by investigating and reporting common -cyber-attacks that each layer is vulnerable to.

Chapter 4 Introduce by illustration a common IoT devices in Smart Home. Also, this chapter introduces three real-world case studies and applied the proposed risk assessment framework to those case studies by looking at the threats and the possible impact of those threats on IoT devices in Smart Homes.

Chapter 5 Firstly provide a generic mitigation approach for IoT devices in Smart Home. Secondarily suggest suitable countermeasures for the layered architecture and the three real world cases. Thirdly propose new and more secure design of layered architecture.

Chapter 6 Form the conclusion to this thesis. Provide recommendations. Set the direction for future research in the field of IoT devices in Smart Home. List the limitations this project has been subject to**.**

2.0 Literature Review

2.1 Introduction of Smart Homes and IoT devices

Smart Home can be defined in several different ways:
From a technical point of view, a Smart home can be defined as “connected sensors, home appliances, and smart devices that connect to the Internet to achieve remote monitoring or remote access to, and remote access of a residential environment.” [2].Smart Home could be described as a bunch of small computation facilities that “identify and deliver personalised services to users who interact and exchange information with the environment” [2].

Smart Home can also be defined as home that is automated, vie the application of the “IoT paradigm, and capable of reacting to the requirements of its inhabitants, providing confirm and security” [8].

Furthermore, from a social perspective Smart home can be defined as a smart environment that is “sensitive and adaptive to modern human and social needs” [2].

As seen from the above definitions, Smart home focuses on automation and control of all the IoT devices in Smart Home, such as control and automation of heating, ventilation, control of devices, the safety of home residents, and home security [2]. However, the main purpose of the Smart home is to “expand the functionality of the first version of the Internet by increasing the ability to connect numerous objectives” [2].

By using the IoT model in Smart Home, “users can share both the information provided by users behaviour and the information collected by the connected things in the physical world” [2] as the IoT development process involves different technology, such as ”wireless sensors networks (WSNs)RFID, Bluetooth, NFC, Internet protocol (IP), electronic product code(EPC), wireless

fidelity(WI-FI), sensors and actuators“[2] the key objective of the IoT based smart home is to enable users to ”uniquely identify, signify and control things at anytime and anywhere vie the Internet”[2]

In conclusion to the introduction of a smart home can be concluded that IoT based Smart Home devices can “produce numerous intelligent and autonomous applications and services that offer personal and economic benefit to society” [2] but at the same time, those IoT devices in our smart homes pose new security and privacy challenges in terms of” confidentiality, authenticity and integrity of the data sensed, collect and exchange by the IoT object [2].Those challenges make the smart home being insecure, the researcher aims to describe the advantages of IoT in Smart homes in the next paragraph before moving the disadvantage and the risks of IoT-based In Smart Homes.

2.2 Advantages of Smart Home and IoT devices

Smart Home has many advantages and can significantly improve the quality of life of individuals, such as detecting emergencies, home safety, finding things easily, homes security, energy consumptions management and interacting with appliances[9].

Basically, there are so many benefits that can be derived from Smart Home and IoT, but if and only if it is used in a safe IT environment. The Cyber Security of Smart Home and IoT devices is a crucial component of the future of Smart Home developments as IoT devices must be able to protect the confidentially, integrity and availability of information.

Smart Homeowners need to be ensured that the IoT devices are secure, as the near future predict, consumer may not be longer having the option to purchase dishwasher, fridge, washing machine or oven without IoT capabilities.” This creates the expectation that nearly all home appliances will be equipped with IoT technology in the future” [10]. However, manufactures should be creating those IoT devices with security in mind, by making sure they are secure before been sold to the end user not just aiming to push the product to the market as soon as possible for higher turnover. Furthermore, this project aims to educate users about all the positives and negatives aspects of IoT devices in Smart Home. The next section in this chapter will focus on the architecture of IoT devices in Smart Home, then the concerns and threats of IoT devices in Smart Home will identify and describes.

2.3 Smart Home architecture

Smart Home architecture is not standardized. Therefore, a generic architecture model has been selected and presented in Figure 2-1 as interoperability standards are missing [11].

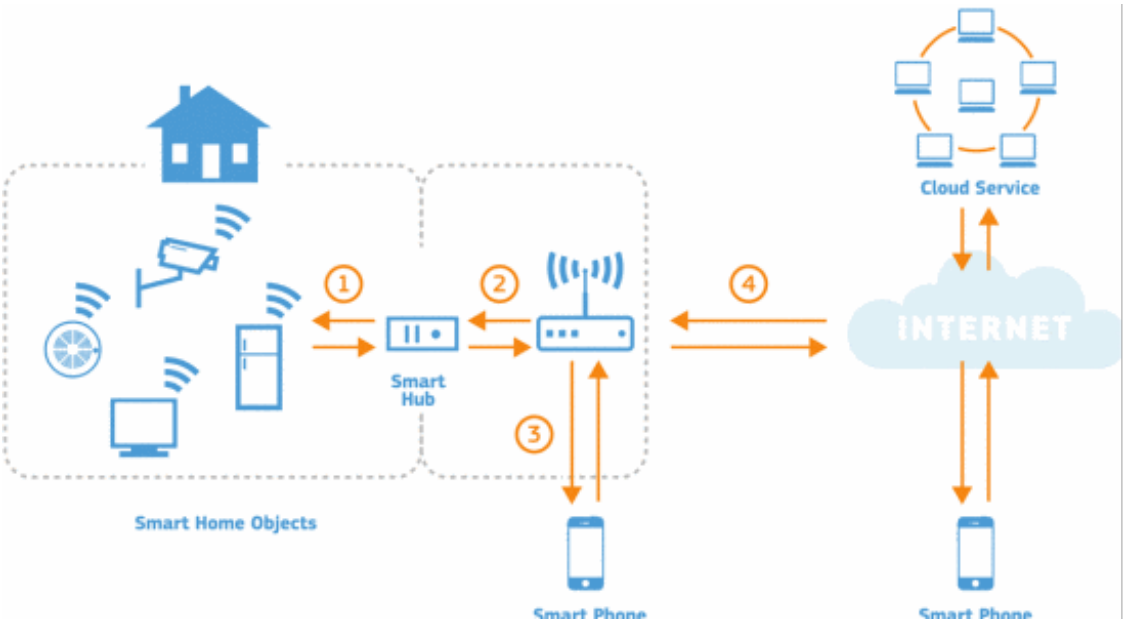

Figure:2-1 Architecture of Smart Home [11]

The architecture model in figure 2-1 shows how the IoT devices in the smart home are organised in islands and how they connect to a Smart hub, therefore the smart hub is responsible for providing connectivity, usually wireless. The smart hub is then connected to the home router via wi-fi interface [11].

The Smartphone user can interact with the IoT devices in two different ways:
Directly and Indirectly -Directly by connecting to the hub and using the connectivity that the hub provides or indirectly by accessing Internet cloud services which will interact with the IoT hub and the connected IoT devices [11]. According to [11] the two different ways of communication are often mixed" to support local and remote interaction" with IoT objectives [11].

IoT Management -In order for IoT management to be possible, a procedure of correlating devices first needs to be performed. Usually, action such as pressing the button on the smart hub will connect the devices to the hub. Once the initial connection is done, IoT management can be carried successfully regardless of the location of the IoT devices [11].

Furthermore, IoT devices support protocols such as Simple Service Device (SSDP) to “unable the transparent configuration of the smart home devices in plug and play mode that required minimum user interaction” [11].

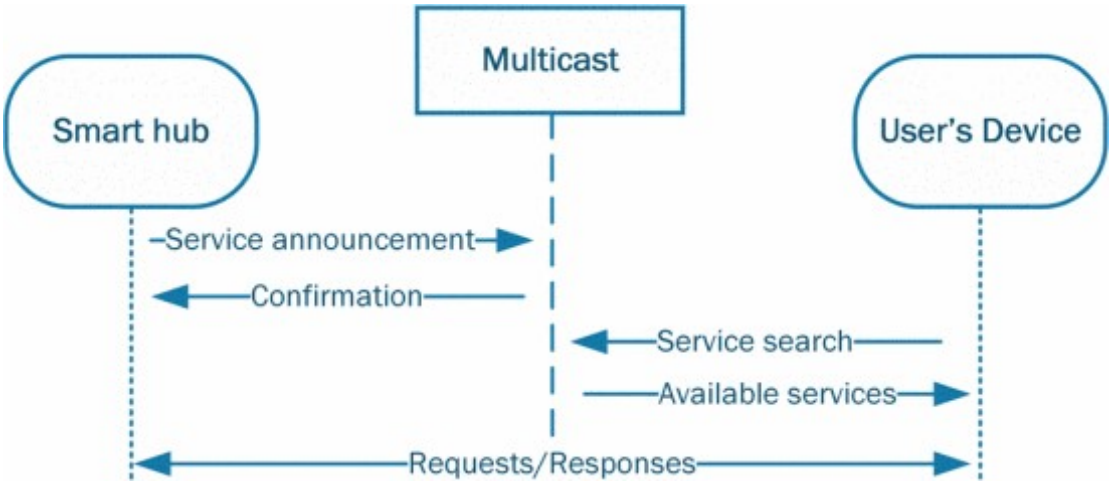

Figure 2-2 Plug and play architecture for smart house [11]

An example of how the plug and play mode architecture works could be:
A user wants to control the heating in his house while he is outside of the house, to do that, firstly, the correlation procedure needs to be completed otherwise the remote access will not be possible. Secondly, the request needs to be launch on the user's mobile phone, and the request needs to be able to reach the cloud service, which forwards it on behalf of the user to the hub that is responsible for controlling the heating in the house[11].
Using a reverse communication channel that is kept open, through the house router, by the hub itself. “As soon as the hub receives, such a request, it sent its correspondence command” [11] to the heating device to receives back their response and forwards it to the user via the cloud service.

2.4 Security Concerns of IoT devices Based in Smart Home

The development of IoT technology for Smart Home with automation and control processes present new security challenges [2]. Thus, the IoT-based Smart Home” requires a new level of security requirements”[2] as the IoT devices in smart homes will contain important, sensitive, and private information. Therefore, when a home user makes the decision to bring IoT devices into their home, the privacy, and the security issue of those IoT devices should be a priority, as IoT devices in Smart Homes are highly vulnerable to attack via the Internet. However, this thesis aims to tackle the problem of IoT-based Smart Home security risks. The next section of this chapter will look at the Smart Home threat model.

2.5 Smart Home Threat Model

The Smart Home Threat model should consider two types of adversaries: Internet and external "entities that can act maliciously on a passive or on the active way depending on their goal"[11]. By internal adversaries is meant someone located close to or inside the Smart Home. On the other hand, external adversaries could refer to someone that is far away and can interact only via the Internet connection [11]. In both cases, "adversaries target either the Smart Home's infrastructure or the information store in the related cloud service"[11]. In the context of the Smart Home Threat Model. Passive adversaries will try to "eavesdrop available communication"[11] that will allow information to be captured and used to monitor user's behaviour or the captured data can be stored and exploited in a later step of an active attack [11].When the adversary is trying this type of attack, he/she will try to "capture the traffic in the different points of the smart home architecture depending on their capabilities and goals"[11]This type of attack affects Smart Homeowners confidentiality and privacy because if adversaries can monitor the communication of the IoT devices in the Smart Home, the adversaries can identify which entities the smart hub communicate with, then identify the habits, and daily lifestyle of the smart homeowners, also the adversary will be able to identify when a smart homeowner is at home and when they are out of the house.
This is concerning, as though eavesdrop attackers not only can monitor and collect data of the IoT devices in somebody else's Smart Home, but also will know when Smart Homeowners are in or out of the house therefore, this type of attack can help adversaries to get physical access to somebody else house.

On the other side, "an active adversary will interact actively with the IoT components, instead of only eavesdropping the underlying communication. He could identify the existence of components by generating the appropriate probes through different network devices "[11], and then possible he will be able to" impersonate a legitimate user in order to gain access to the smart device"[11]. The consequences of such an attack are breach of privacy and confidentiality as well as data integrity and unauthorised access and ultimately disturb functions of the provided service.

So far, the researcher has identified what adversary is able to achieve if he applies a passive or active method of attack. However, that not all as the [11]describe adversary can combine the passive and active attack, and that is where the adversary can have an immediate impact on user safety. A good example is a situation in which an adversary attacks a smart socket that provides electricity to a health device" if the adversary knows the unique identifier by eavesdropping the communication traffic, he could cause a denial of service to the IoT that could have an immediate impact on the user safety" [11].

Besides the passive, active, or combine attacks that an attacker can execute on the network layer to impact smart home user confidentiality, privacy, and safety as well as gain unauthorised access to IoT devices based in Smart Homes. It is another very important aspect that needs to be added to the Smart home list of threats before the end of this chapter, and that is software vulnerabilities of IoT devices, and this is simply because, as the author [11] has described the IoT devices in Smart Home "relies on a lightweight version" of well-known operating systems, that adversaries are looking to exploit with very few resources [11] .

However, as one of the goals of this project is to identify and describe the cyber security attacks that IoT devices based in Smart Home are vulnerable to, the next chapter is dedicated to the different types of attacks.

Chapter 3 Different types of attacks in IoT based in Smart Home

This chapter aims to identify and describe the different types of attacks that IoT devices in a smart home are vulnerable to, but before the researcher dip into the details of those cyberattacks, a more general overview of the layered architecture of IoT will be provided. Figure 3-1 represent a generic architecture of IoT systems [11].

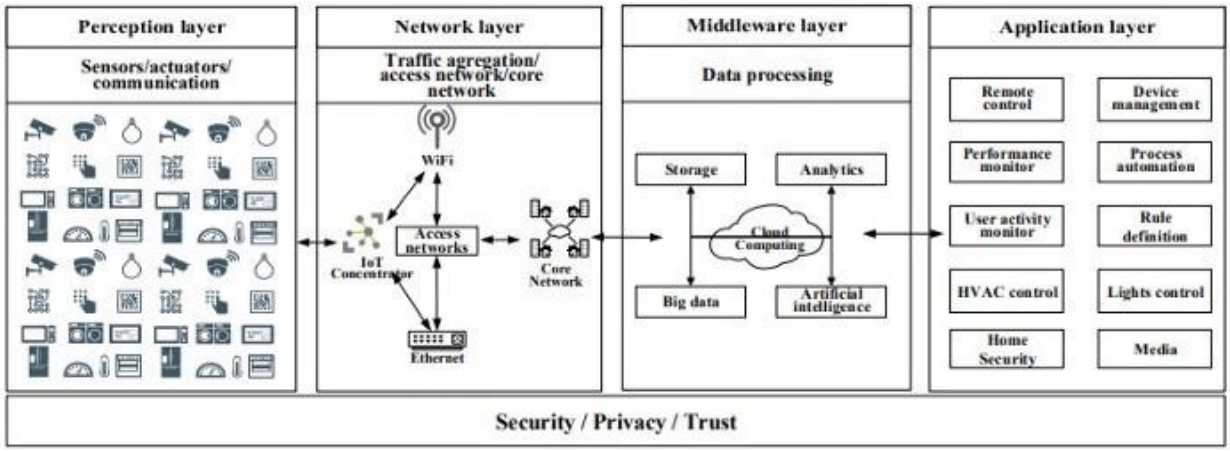

Figure 3.1 represent a generic architecture of IoT systems [11]

Furthermore, figure 3-1 also illustrate the technical details and the four different layers of the IoT architecture, which are Perception Layer, Network Layer, Middleware Layer, and Application Layer.

The researcher aims to describe each layer with details before moving to the next section of this chapter which is IoT-based Smart Home cyber-attacks.

Perception layer- also called the physical layer, which has the sensors for sensing and gathering information about the environment [13] the main purpose of this layer is correspondence between the different physical IoT devices and provide" authentication of devices and service to upper layers"[14].

Network Layer – is responsible for connecting other IoT devices, networks, and servers. Therefore, with the assistance of the wireless sensors, the main goal of this layer is to assemble information that is given from the physical layer and sent it to a central processing unit. An example could be a single smart device in our smart home sent a message to the network, and the network layer" carries exchange of the data on the systems of IoT. This secure and reliable exchange of information is done by this layer from perception layer and toward different layers" [14].

Middleware Layer- the purpose of this layer is to merge the service of the perception and the network layer; therefore, this layer performs an intelligent processing function**. Application Layer**- "it is a presentation and service layer where the data collected by the devices are employed, understood and shared as well as their results can be observed" [15], furthermore

the application layer can be configured in different ways according to the service provided [15] as shown in figure 3.1 IoT devices architecture and figure 3.2 shows an IoT protocol according to the layers.

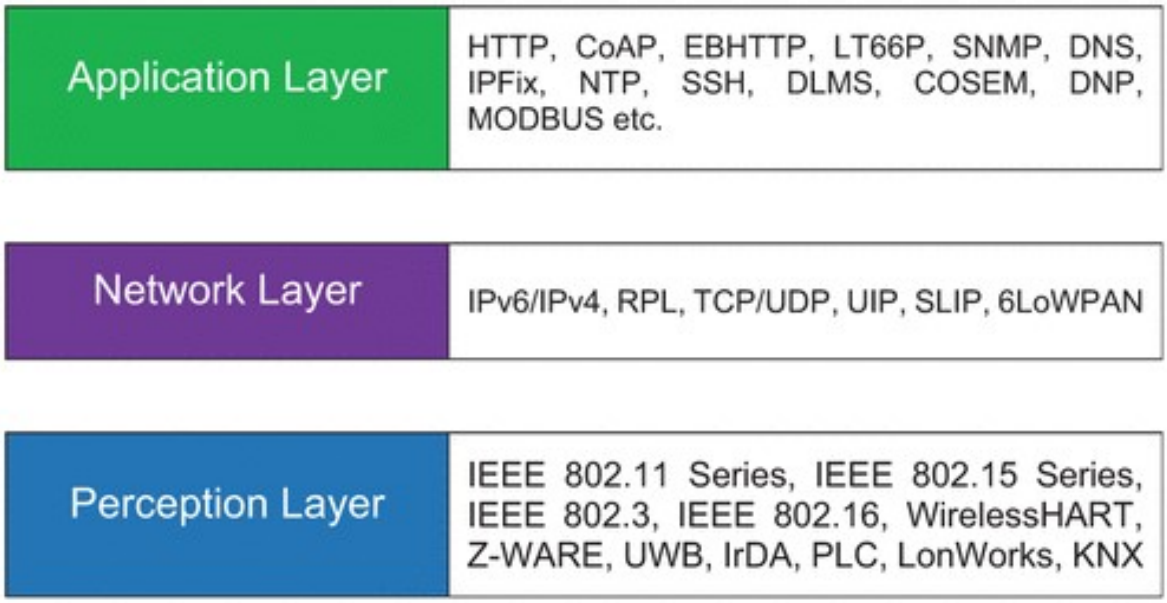

Figure 3.2 IoT protocol according to the layers [16]

Furthermore, this chapter aims to describe the cyber-attacks on IoT Based Smart Home that is performed on each layer and in the next chapter risk assessment framework will be applied.

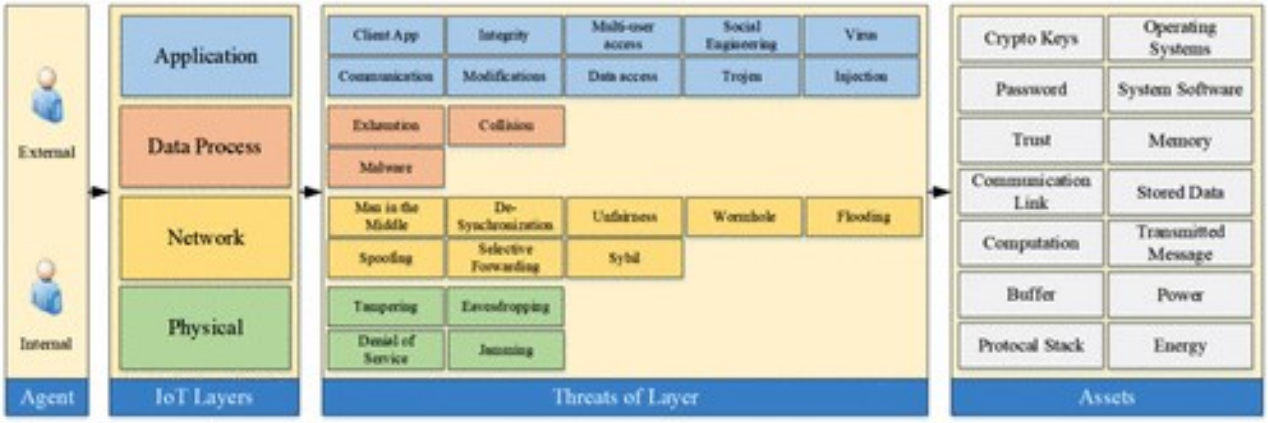

Figure 3.3 Threats classification according to the IoT layers [16]

As shown in Figure 3.3 attacks on IoT platforms are classified as physical layer attacks, network layer attacks, data processing layer attacks and application-layer attacks.

The rest of the chapter will focus on the four layers and the associated cyber-attacks at each layer.

3.1 Physical Layer attacks –is where “object, sensors and actuators take place in data generation.” [16]. Moreover, the physical layer of IoT is targeted by attacks such as tempering, eavesdropping, denial of service (DoS) and jamming [16]. It is worth to be added that the sensors are the most vulnerable since they can easily be exploited, as the sensors are the once that collect data directly. Most of the causes, sensors are targeting by attacks of tempering and jamming [16].

3.1.1 Tempering Attack -in this type of attack, “the hardware or software features of IoT objects are modified by the attacks vie physical or cyber methods” [16]. Therefore, tempering attacks can violate fundamental security policies such as privacy, availability, and integrity of the home system. Furthermore, a successful tempering attack will enable the attacker to gain direct access to all IoT objects [16]

3.1.2 Jamming Attack – In this type of attack, the data integrate is damaged by interfering the network traffic during the communication of the sender and receiver object.[16] Figure 3.4 Illustrate in detail how a jamming attack is performed.

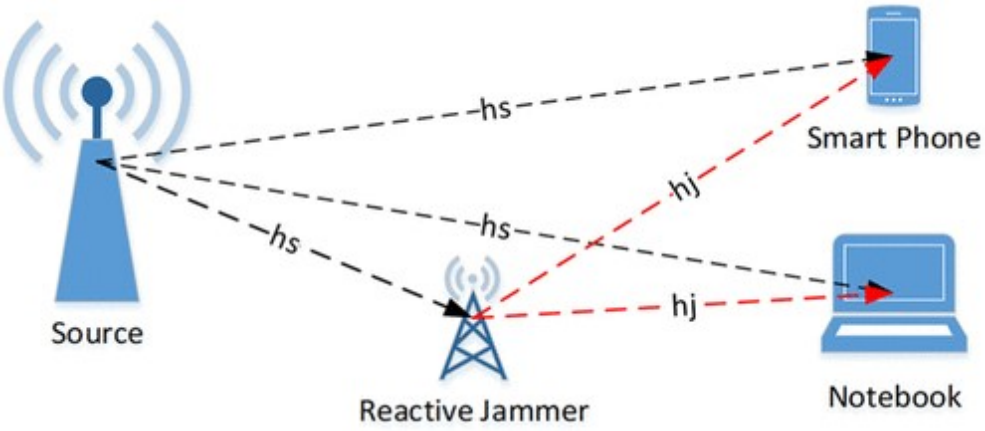

Figure 3.4 Jamming attack [16]

In, fact jamming attacks are one of the “most dangerous types of attacks as are used to block the IoT network and data exchange between IoT objects communicating wirelessly” [16]. Jamming attacks will target the accessibility of IoT systems.

3.1.3 Eavesdropping attack – is a technique that is used to “access and retrieve the communication traffic between IoT objectives”[16]. This type of attack targets the confidentiality of a system.

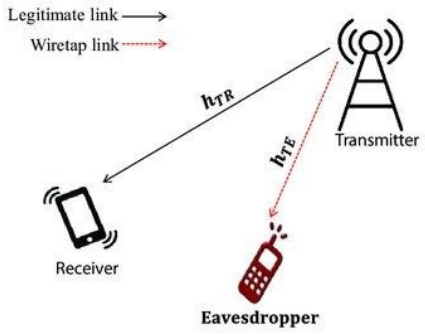

Figure 3.5 Eavesdropping attack [17]

3.1.4 DoS attacks – are made to disturb the services of IoT, as the communication network between objects is blocked, and the result is not communication after all. DoS attacks can target “all the physical data link, network transmission and application layer of TCP/IP”[18]as shown in figure 3.6 attacker get control “of the target systems by sending a continuing request to the target IoT platform from a different location using the computers he has convert to zombies”[18]. However, the main point is DoS attacks target the accessibility of IoT.

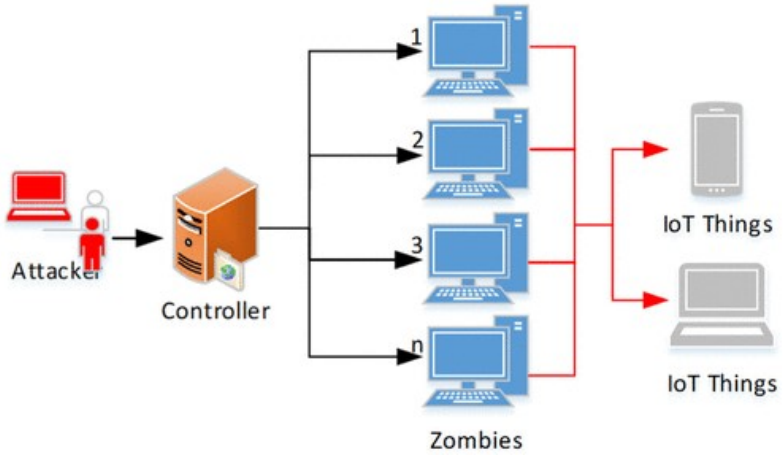

Figure 3.6 Denial of service attack

3.2 Network Layer Attacks -are happening in real time, the attacks are performed when the “data collection and data processing are carried out”[18]. The cyber-attacks that are carried out

on the network layer are: MITM, Spoofing, Desynchronizing, Selective forwarding, Unfairness, Wormhole, Sybil, and flooding.

3.2.1 Man in the Middle Attack- "capture, read and modify data"[18] between two communicating IoT devices, as figure 3.7 illustrate.

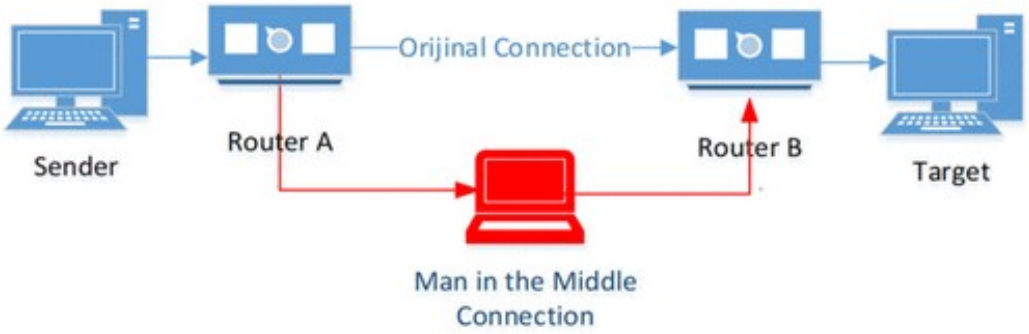

Figure 3.7 MITM attack

The main goal of MITM is to "change the data content by capturing and replacing the data packets on the IoT platform vie sabotaging the traffic"[18]. MITM attacks have a high rate of success with Smart Home devices because there is a lot of neglected, open, and uncontrolled IoT devices in Smart Home.

3.2.2- Spoofing Attack- happened when an attacker "emulate, modify or resent IP address or transport protocol information such as UDP and TCP ports to poison network traffic"[18]

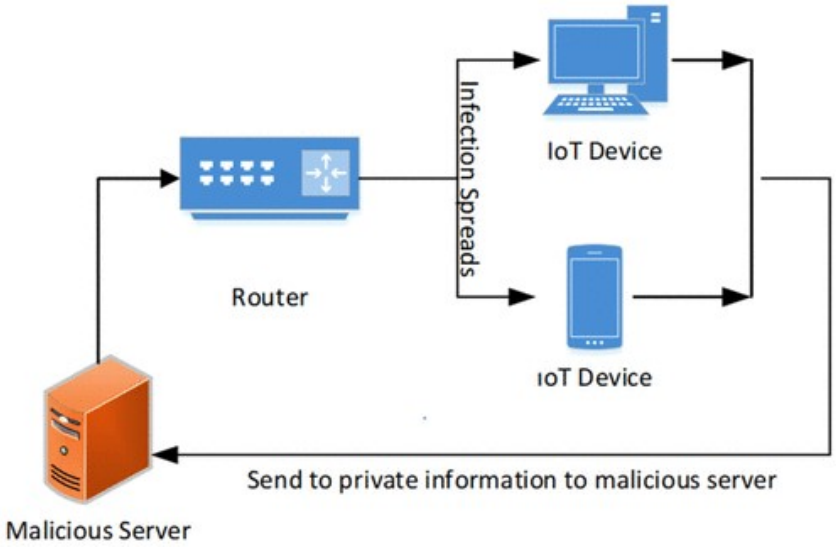

Figure 3.8 Spoofing attack [18]

As figure 3.8 shown, the attacker needs to generate “rooting nodes, extended or shortened transmission path and false error messages[18] Therefore spoofing attack targets the integrity of a system.

3.2.3- Desynchronizing Attack - is a wireless communication attack, as IoT objectives in Smart Home use mostly wireless communication, the way in which this type of attack works is ‘interfering with communication parameters”[18] causes network traffic not to work properly.

3.2.4- Selective Forwarding Attack - IoT devices in Smart Home required multiple routing for communication between objects. “A node seized by an attacker can change network traffic by reducing some data packets and redirecting to different locations”[18]. As result of selecting forwarding attack, the data that should reach its target may be missing or corrupted[18]

3.2.5- Unfairness Attack – “is a repeated collision attack, that aims to disturb the equal load sharing mechanisms of wireless sensor networks (WSNs)”[18]

3.2.6- Wormhole Attack-in this type of attack that the attacker sent packets” at a point in the network to other points on the network through the tunnel and then send them back to the network from there”[18]

3.2.7- Sybil Attack- is performed on devices with multiple IDs to generate “multi-source and distributed network traffic” although nodes are fake, they can act as real nodes. Therefore, Sybil attacks “manipulate fake abuse pseudo-identities to compromise the effectiveness”[18] of IoT devices.

3.2.8- Flooding Attack-can reduce the speed of traffic between IoT devices or stopping the network by occupying the hub. Figure 3.9 illustrate DNS flooding attack, where the volume of request disturbs the services of the “DNS service provider and prevent real users from accessing their DNS servers” [18]

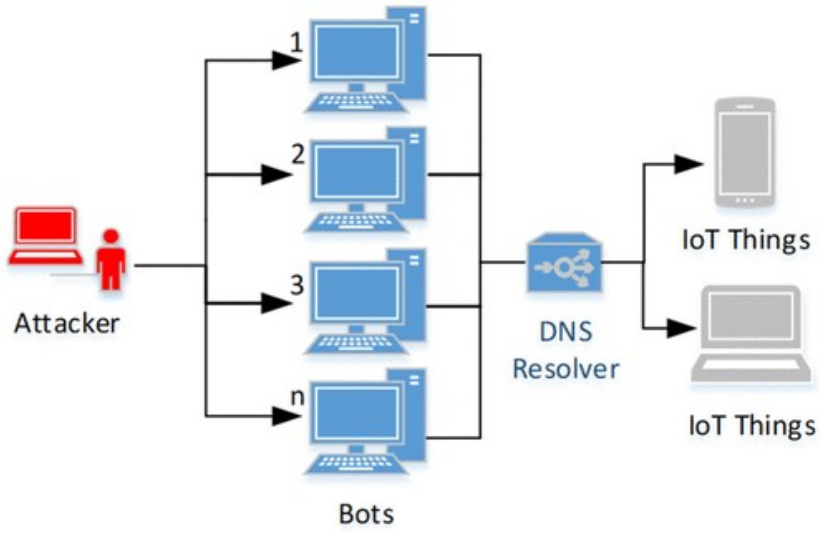

Figure 3.9 Flooding attack [18]

3.3 Data Processing Layer Attacks – in this layer, the data is collected using sensors which are generally processed in cloud systems ", and this process generates the data processing layer"[18] The attacks on this layer are performed by using malware that is embedded in the data from the sensors.[18]

3.3.1 Exhaustion Attack- "aims to interrupt the data processing of the IoT infrastructure"[18] According to [18] exhaustion attacks are not very common, especially when Smart Home devices are using cloud -based systems, because in the cloud -based systems protective measurements against exhaustion attacks are easily implemented.

3.3.2 Malware Attack – in the data processing layer, generally malware will refer to viruses and Trojan horses, as the malicious software is injected into that data of IoT devices "in order to grant access for seized cloud or distributed systems"[18]. According to researchers[17], malware attack is difficult to detect or prevent, but the issues of those preventions and detections methods will be discussed in Chapter 4 of this project.

3.3.3 Collision Attack -is a jam-type of attack, and the intended purpose of this attack is to make the network unusable.[18]

3.4 Application Layer Attacks– is the layer, where user communicates with the IoT platform. The application layer performs several tasks such as "report generation, querying, analysis, visualization of the data, authentication and interaction with IoT"[18].
In fact, the application layer generates a large amount of data, and due to this it becomes difficult to be secure, therefore this layer poses a challenge to smart homeowners in terms of

cyber security. Furthermore, this layer experience some of the following cyber-attacks; Client application attacks, Communication attacks, System Integrity, Modification, Multi-user Access, Data access and Social Engineering. This chapter will be concluded by looking at each of those attacks in detail.

3.4.1 Client Application Attack - happened when devices used HTTP, as malicious software can infiltrate the IoT systems vie client site, and those attacks may remain in passive mode and "cause faulty production on the output of the system"[16]

3.4.2 Communication Attack - is performed when the IoT platform is weakened by gaining access to the configuration interface or commination channel.

3.4.3 System Integrity Attack – occur when data from the IoT device is accessed without an authorization from the owner of the device, however as researchers has identified the main aim of the integrity attack is to modified data and perform operation without the knowledge of Smart Homeowners. System Integrity attacks are serious threat that need to be addressed immediately, as those type of attacks can be life threatening. In a situation where the IoT device that have been accessed is closely related to the health and wellbeing of an individual.

3.4.4 Modification Attack – can occur due to changes of systems, configuration, or environmental changes.

3.4.5 Multi-User Access Attack – can occur when the configuration of the IoT system is changed by the user, therefore the "simulations operation of the configuration files and the simulations operation of the configuration changes can cause a conflict of updates"[18]

3.4.6 Data Access and Security Measure -need to be implemented when updates and configuration changes had taken place, as the owner of the IoT devices needs to make sure the right level of access is given to those devices, otherwise privilege level could be escalated.

3.4.7 Social Engineering- can be defined as an act of capturing and manipulating user's confidential information such as date of birth, passwords, banking information, address, national insurance number and so on, basically any information that can be used to identify an individual can be beneficial to an attacker. Today the threat area of social engineering attacks has expanded even further and now covers IoT devices in Smart Home.
An example of an IoT social engineering attack In Smart Home has been illustrating in figure

3.10 in which an attacker has compromised a smart meter that is connected to the cloud.

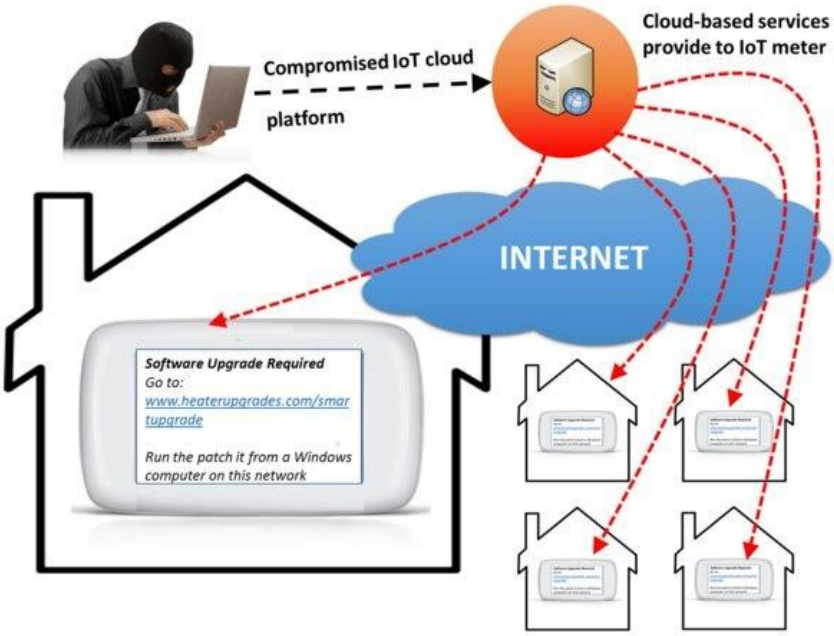

Figure 3.10 Smart Meter phishing attack vie compromise update and content service in the cloud[19]

In the illustrated above IoT attack, the attacker can monitor “unencrypted communication between the cloud service and the smart meter and inject information into existing data flow, or potentially sent a direct message to the meter in this way the attacker has gained complete control over the cloud environment”[19]. Regardless of which of the two above cases the attacks have applied, a message will pop up saying Software Update required with the instruction an update to be run from a computer and if user decide to follow the instruction, they will be phished.[19]

This chapter has identified the layered architecture of IoT as well as described the common cyber-attacks that each layer is vulnerable to. Table 1: Include summaries of the Layers and the types of attacks that each layer is vulnerable to.

Layers	Attacks
Physical Layer	• Tempering • Jamming • Eavesdropping • DoS
Network Layer	• Man-In-The-Middle-Attack • Spoofing • Desynchronizing • Selecting Forwarding • Unfairness • Wormhole • Sybil • Flooding
Data Processing Layer	• Exhaustion • Malware • Collision
Application Layer	• Client Application • Communication • System Integrity • Modification • Multi-User Access • Data access and security measures • Social Engineering

Table 1: Summaries of the attacks that each layer is vulnerable to.

The next chapter in this study aims to introduce the various IoT devices in Smart Home, suitable risk assessment methodology and real-world examples of vulnerable IoT devices in Smart Home. Furthermore, the next chapter will also provide a suitable countermeasure that can be applied to those real-world examples.

Chapter 4 Risk Assessment and Case studies

This chapter aims to introduce a risk assessment framework for IoT devices in Smart Home and further develop best security practices. Also, this chapter aims to support its recommendations by introducing relevant case studies and applying a suitable framework to those case studies.

4.1 Introduction to IoT Devices in Smart Home

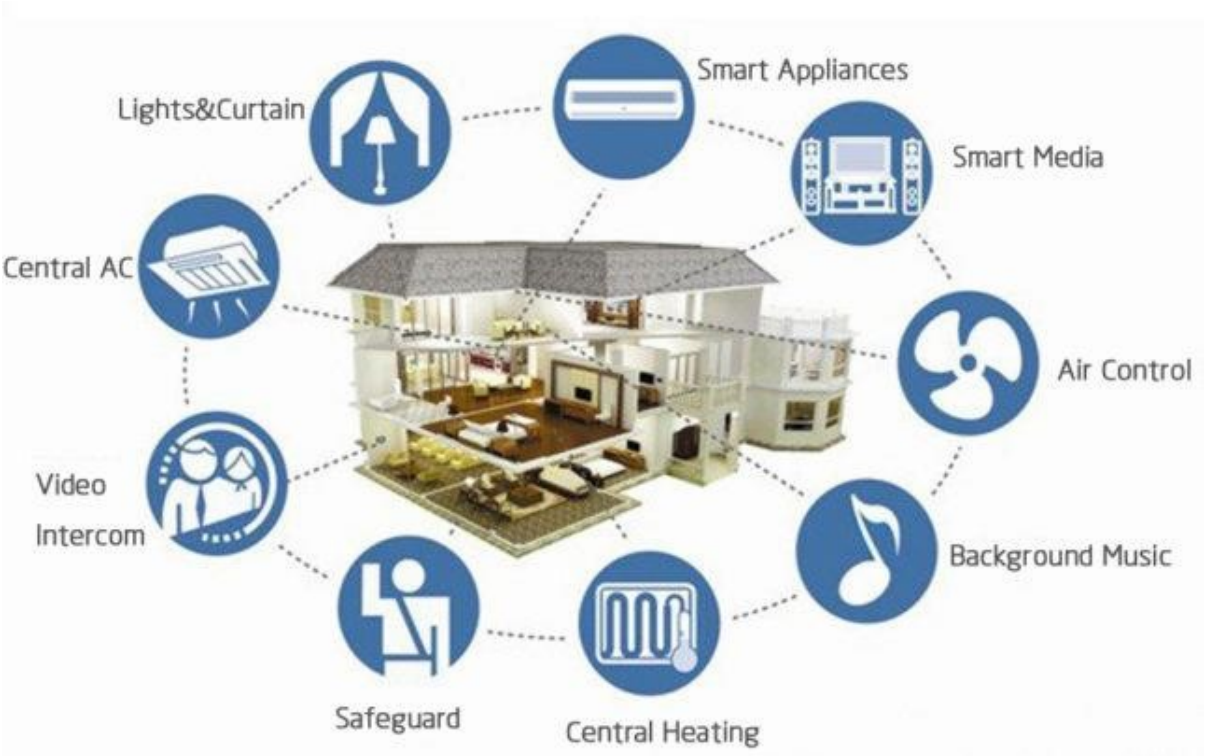

Figure 4.1 Introduction to IoT devices In Smart Home

IoT in Smart Home has brought Innovation, Convenience, Security and Efficient Use of Energy to Smart Homeowners. However, IoT in Smart Home has also introduced many challenges related to the privacy and security of those IoT devices, and as the researcher has identified earlier those IoT devices are vulnerable to many different types of cyber-attacks.
Therefore, this chapter also aims to educate End users, IT Consultants and Manufactures of how to apply appropriate security and privacy measures vie a risk assessment framework to everyday IoT devices in Smart Home.

4.2 illustration of Everyday IoT devices in Smart Home

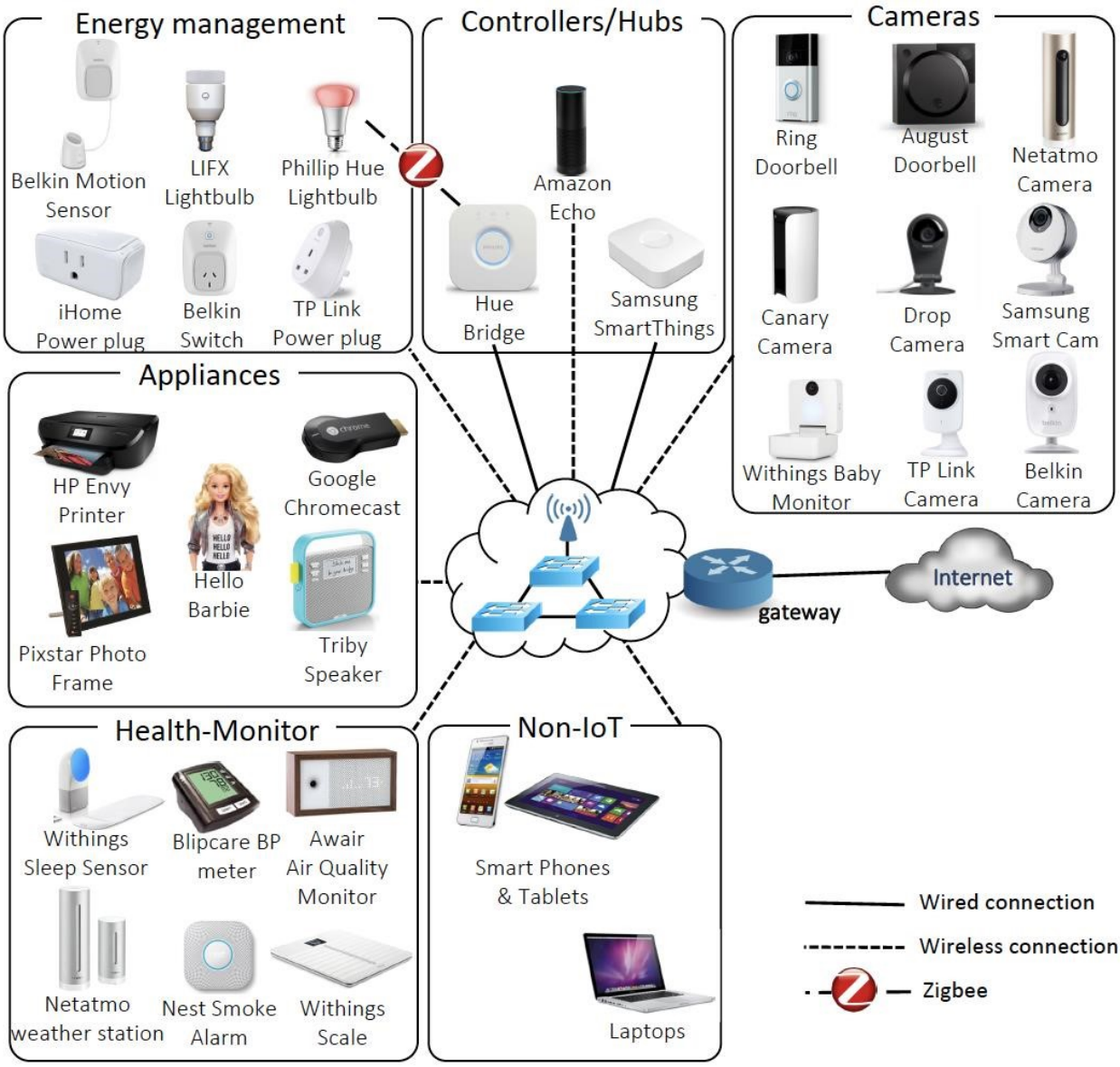

Figure 4.2 illustrate some of the common devices in Smart Home [20]

IoT Device in Smart Home will collect, store, and communicate user sensitive and private information. Furthermore, those devices can give access to physical premises to unauthorized users. However, in 99.9 per cent of the cases Smart homeowners will still blandly trust those IoT devices, hopelessly hoping the manufacture of these devices has taken into consideration the security of those devices. But as the researcher has identified those Smart devices are not that smart overall as they are highly vulnerable to different attacks such as eavesdropping, impersonations, DoS, software exploitation and many more.

4.3 Risks of IoT devices in Smart Home

4.3.1 Understanding Risk

IoT devices in Smart Home could carry potential risks associated with privacy and end users need to be able to protect their IoT devices in a home setting. They need to be able to understand the main concept of risk and how risk is measure and managed.

Firstly, Risk can be defined as a measure of the "extent to which an entity is threatened by a potential circumstance or event and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence"[21].

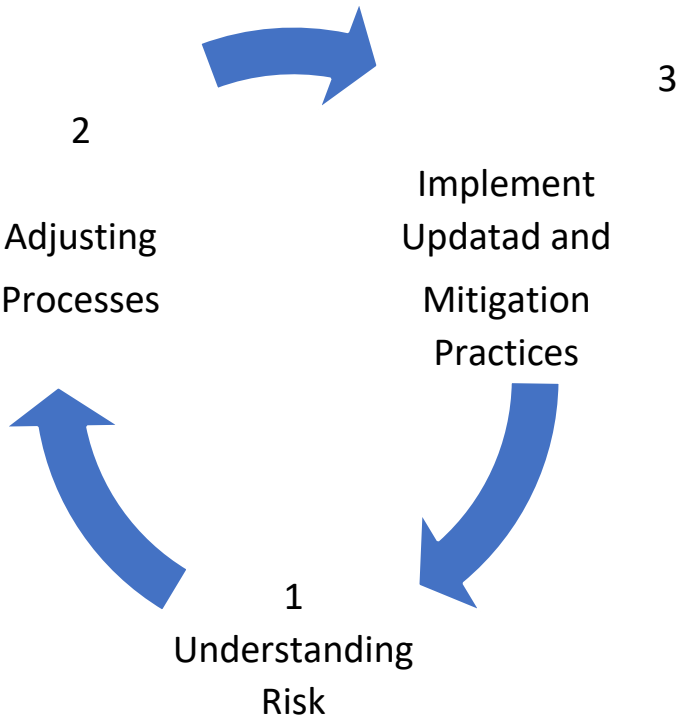

Figure 4.3 General Risk Framework Smart Home

Secondary, users can consider that IoT devices have been compromised when one or more of the following abilities of the systems has been lost. Such as loss of confidentiality, loss of availability and loss of integrity.

Figure 4.4 When IoT device in Smart Home has been compromised!

Therefore, the next section is this project aims to introduce a risk assessment approach.

4.4 Risk Assessment Methodology

The methodology adopted for this research is the OCTAVE Allegro methodology.
The researcher has selected this framework because OCTAVE Allegro allows" comprehensive risk assessment, yield robust results and focus mainly on information assets"[2]. Furthermore, this approach analyses how information is used by the user and the system.

Figure 4.5 Represent an overview of the approach, including the phrases and the individual steps involved within each phrase.

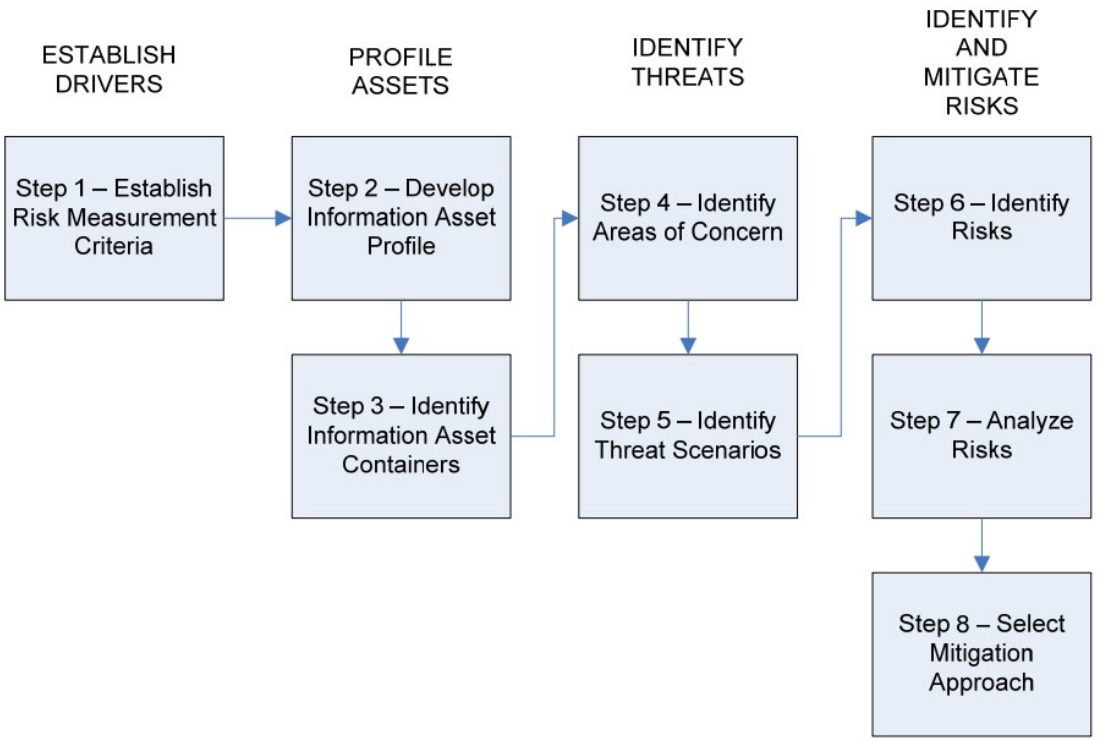

Figure 4.5 OCTAVE Allegro methodology, which consists of eight steps, and four main groups[22]

4.4.1 Establish Driver Phase- the main goal of this phrase is to establish risk measurement criteria for IoT devices in Smart Home, by developing those risk criteria's Smart Home residents will be able to examine the possible consequences if the smart devices are compromised [2].

4.4.2 Profile Assets Phrase – in this phrase which includes step 2 and step 3 "critical information assets are initially identified and then profiled"[2] . At this stage the users of IoT devices in Smart Home need to be able to allocate which devices store what type of data and how data is communicated within devices.

4.4.3 Identify Threats Phrase – include step 4 and step 5 from figure 4.5 and focus on identifying areas of concern and identifying a particular threat scenario. An example of area of concern could be IoT devices in Smart Home that is using default password and an example of threat scenario could be when a malicious party had managed to accessed and manipulated the functions of IoT device in the home setting.

4.4.4 Risk Mitigation Phrase- include step 6, step 7, and step 8 in Figure 4.5. The main goal of this phrase is to determine how risk is identified, analyze and what approach needs to be applied in terms of risk being mitigated.[2].At this stage, Smart Homeowners and users of the system should be able to identify relevant cyber security threats and, they should be able to analyses the possible consequences of those threats.

The next section in this chapter aims to introduce the three real-world case studies.

4.5 Case study 1: Amazon Alexa

Figure 4.6: Amazon Alexa [23]

Amazon Alexa is a virtual assistant AI technology developed by Amazon[24]. The smart IoT device is capable of voice interaction including streaming podcasts, playing audiobook, providing weather forecast, reading news from the Internet, and so on the list of functionalities that Alexa provide is long. However, Alexa can also control other IoT devices in the Smart Home setting and use itself as a home automation system.[24]. Moreover, in Smart Home, Alexa can help residents to order food, play music, update users of sports news and message and call everyone from the user phone book. So far, so good thousand and millions of people want to have Amazon Alexa in their homes and according to Statista, 65 million have been sold so far.[25] as the popularity of Alexa has grown significantly the smart device started to attract the attention of two parties first, the hackers who want to explore the device vulnerabilities and the cyber security researcher who wanted to know more about Alexa and how to make it more secure.

In 2020 Fobes.com come up with a statement warning users to be aware of the questions they ask Alexa.[26] Later on, researchers from Check Point Security had managed to identify a series of vulnerabilities in Alexa, those vulnerabilities shock the users around the world. Simple because users were one click away from been hacked. In the scenario in which users click malicious links directing them to the Amazon website, a hacker will be able to retrieve personal data from Alexa, get victim voice history, home address and full control over their Amazon account.[26]

After the confirmed vulnerabilities, Forbes.com was in the position to warn Alexa's users that every gadget connected to the Internet can become a potential vulnerability to your Smart Home despite the fact it has been produced from such a reputational company as Amazon.

4.6 Case study 2: Samsung Smart Fridge model RF28HMELBSR

Figure 4.7 Samsung Smart Fridge [27]

The smart fridge by Samsung is design to integrate the users' Gmail calendar with its display. The main purpose of the incorporated functionality and connectivity is an efficient food waste management system. However, researchers have discovered and report that the fridge is vulnerable to a man-in-the-middle attack in which login details of the user's Gmail account can be stolen[27].

The Man -in -the- middle attack is possible simply because, Samsung has implemented an SSL certificate to secure the connection with Gmail, but later has been reported that the smart fridge does not validate the SSL certificate. In this way, hackers can get access to the home network and monitor the activities for username and password used to link the fridge to Gmail[26]. Furthermore, to this case study could be said that, apart from the common man -in the middle -attack, the fridge also has other vulnerabilities as it has been hijacked and used in a botnet attack.

In conclusion to this cases study could be concluded that Samsung Smart fridge is vulnerable to the two most common attacks that IoT devices in Smart Home experience. However, mitigation practices of those common vulnerabilities will be provided in Chapter 5.

4.7 Case study 3: Ring Smart Camera

Figure 4.8 Ring Smart Camera [28]

Ring is a home security company owned by Amazon. The company main product is Smart Cameras like the one that has been illustrated above in Figure 4.8

In 2020 Ring reputation of providing home security went down as dozen sue Amazon after hundreds of Smart Home cameras have been hacked.[29]

The accidents that have been reported to the police included but were not limited to, strangers speaking to children through the home cameras, racial abuse to the home residents and death threatening and many more terrifying examples have been reported, and some of them have been even recorded by the home residents as prove.

In a statement, a Ring spokesperson said that hackers are responsible for the attacks, and at the same time the organization denied an accusation that their systems or network had been compromised [30].

Instead of that, Ring tried to blame a smart cameras user, by saying that users have neglected security by reusing the same password on multiple devices and not practicing good password hygiene.

In a following statement, Ring advise smart cameras users to enable two factors authentication and change password regularly in term to stay secure[30]

In response to Ring statement, Orange lawsuit said that “Ring is wrongfully placing the blame on users”[30] and Ring must have a system in place in which users are alerted in a situation where an unknown IP address is attempting to log in to they are home network. Furthermore, Ring should have incorporated better security practices by asking users to log in with a unique account name instead of a log with email[30]

Vice ‘s Motherboard and many cyber security specialists and academics called Ring security awful. A journalist working on the case found that hackers have developed special software for sorting compromised email addresses and passwords and that was the way hackers were able to compromise Ring Smart cameras by applying those compromised emails and passwords [30].

However, that was not all the accusations Ring was facing at the time other lawsuits accused Ring of sharing the footage from their cameras with third parties without the permission and knowledge from its users. Obviously, Ring was not complying with General Data Protection Legislation 2018, breaking the law by exposing the personal information of its users, and due to that Ring was due financial fines.

The next section in this chapter aims to perform a risk assessment on the three real-world cases that have been described so far and present the results in a table.

4.8 Risk Assessment real-world cases

This section is the last section in this chapter, and the aim is to perform a risk assessment exercise on the three real-world cases that have been described in sections 4.6, 4.7 and 4.8. The risk assessment aims to apply the OCTAVE Allegro methodology, but despite the detailed description of the OCTAVE allegro standard, this risk assessment exercise will apply a more general approach and focus on steps 3, 4, and 5 from phrases two and phrases three.

The results in which have been presented in Table 2. In the following chapter 5, the risk assessment exercise will be extended, and phrase four which is the risk mitigation phrase will be applied to the real-world cases.

Step 3 in OCTAVE Allegro: Identification of the device	Step 4 in OCTAVE Allegro: Area of concern and vulnerabilities	Step 5 in OCTAVE Allegro: Identifying treats scenarios, the possible consequences
Amazon Alexa	• Misconfiguration (CORP) • Cross-Site Scripting	• Misconfiguration -allow hackers to perform actions on the victim behalf and view personal data [31] • Using XSS able to get CSRF token. • Hackers can install and delete commands and apps • Obtain voice history of users
Samsung Smart Fridge	• Man in the Middle attack • DDoS attacks	• Steal sensitive data, in this case, is Gmail login information • Malicious parties can get full access to the system • Malicious parties can add back door • They can change the configuration of the system • Impersonation • DDoS attacks –devices are being used as a zombie, without the consent of smart Homeowners. • IoT devices used in DDoS attacks have slower processing speeds.

Ring Smart Cameras	• Unauthorised access to Smart Home • No authentication • Sharing data with third parties' and lack of Compliance with GDPR • Poor security Practise	• Unauthorised access - to the cameras allow Racial abuses. • Surveillance and Privacy Violation as well as Verbal Threatening of Smart Home Residents. • Malicious parties have been able to monition and talk to children without the knowledge and the permission of the parents • Financial loss from robbery as hackers can monitor when owners are at home and when they are not. • No authentication allows any devices to connect to the home network without the knowledge and the permission of Smart Home residents. • Sharing information with a third party without the consent of users means not compliance with GDPR • Ring applied a poor security practice to its cameras as email and password have been used as log in instead of a unique authentic number

Table 2: Risk Assessment OCTAVE Allegro step 3, step 4 and step 5 applied to: Amazon Alexa, Samsung Smart Fridge and Ring Smart Camera.

The next chapter in this project will introduce readers to the countermeasure of the Smart Home by layered architecture and the three real-world case studies.

Chapter 5 Countermeasures: Smart Home Implemented Update and Mitigation Practices in Layer Architecture.

IoT devices in Smart Home need to maintain a high level of security at all the time to stay secured against the various cyber-attacks. This chapter aims first to propose a general mitigation approach for Smart Home by applying Profile Asset Phrase of OCTAVE allegro framework and particularly step 2, which is identifying assets and providing a possible mitigation approach to the identified assets.

Secondly, this chapter aims to advise users on how to secure the layers in IoT architecture.

Furthermore, this chapter aims to refer to the three real case studies from chapter 4 and provide a mitigation strategy to the vulnerabilities and threats found in those cases.

5.1 General Guide: Identifying Information Assets in Smart Home and Possible Mitigation Actions

Step 2 in OCTAVE Allegro: Identifying Information Assists	STEP 8 in OCTAVE Allegro: Possible Mitigation Approach
User Credentials- can be compromised at any time through various attacks such as Man in the Middle and the case of Samsung Smart Fridge	• Implementation of multi-factor authentication • If fusible implementation of biometric identifier • Users need to be aware of social engineering technicist
Log In Information Amazon Alexa vulnerabilities allow the login information to be stolen from Alexa	• Secure the physical location of IoT devices in Smart Home • Replace default passwords • Replace default configuration • "Provide secure access to devices configuration interfaces"[2]
Wireless Internet Connection Smart Home	• Wi-fi connection needs to be secure, as unsecured wi-fi will expose user's personal data • IoT devises management systems need to be implemented before using home automation applications such as Alexa. • Be aware of lost or stolen devices

Ring Smart Camera or any other smart camera that is part of the Smart Home settings	• Making sure only authorised users have access to the video cameras control panel • Avoid third-party outsourcing where possible this will reduce uncontrolled data sharing. • Change default settings on the IoT devices to improve the security level of those devices.
All the other IoT devices in the house.	• Use only secure communication channel • Limit network traffic and permission to authorised users only

Table 3: General Guide to Smart Home security and possible mitigation actions

The next step in this chapter will look at the layered architecture of IoT and provide general but useful advice to Smart Home residents on how to make Smart Home IoT architecture more secure.

5.2 Securing the layers of IoT in Smart Home settings

5.2.1 Physical layer - is the layer where all the sensors employed, sensor like RFID, Bluetooth, wireless sensors, and protocol such as LTE [16].However, the countermeasure of the physical layer will focus on five main areas which have been described in 5.2.2,5.2.3, 5.2.4,5.2.5 and 5.2.6.

5.2.2 Device Authentication – when a new IoT device is brought home, and need to join the home network, the device needs to authenticate itself first and the reason for that is, the network will be able to identify which IoT devices are part of that network and which IoT devices are not part of that network in this way malicious devices can be kept out of the network.

5.2.3 Secure Booting- as known IoT devices relay of lightweight software due to limitations related to the computation power of those devices therefore many cryptographic algorithms cannot be implemented, but some cryptographic algorithms such as NW and WH are suitable for IoT devices with low utilization of power[32].

5.2.4 Data Confidentiality – in terms of data to remain confidential when IoT devices are used in Smart Home setting, data need to be encrypted before data been sent. In this way, data will remain confidential even in a situation when a malicious party has captured the data, the data will be useless to the hacker as will be unreadable. However, as mentioned above, applying encryption algorithms to IoT devices is a challenge and strong encryption algorithms such as AES cannot be applied. According to [32] RSA will be more suitable for IoT devices, but it is seen as a doubtable solution.

5.2.5 Data Integrity – "to avoid the tempering of sensitive data the technique of error detection need to be provided at each physical device"[32], Such as Cyclic Redundancy Check (CRC).

5.2.6 Data Privacy – can be provided to the physical layer by applying one of the following encryptions algorithms DSA, RSA, BLOWFISH and the reason for that is because those algorithms have less consumption of power.[32]

Physical Layer: Security Countermeasures	Implementation Mechanism
Device Authentication	Devices need to authenticate themselves before joining a home network
Secure Booting	NW and WH
Data Confidentiality	RSA
Data Integrity	Cyclic Redundancy Check (CRC)
Data Privacy	DSA, RSA, BLOWFISH

Table 4: Summary of Physical layer: Countermeasures and Implementation Mechanism

Furthermore, anonymity and hiding of private information like "address and location are very important for confidentiality Zero-Knowledge techniques could be the best solution, but it has a drawback that has a large processing power because of strong algorithm it cannot be implemented" [31] on a device with such a low consumption power as the IoT devices in Smart Home. However, as [32] recommend K-anonymity is the best approach for less power physical devices in IoT network.

In conclusion, this layer has experience tempering and eavesdropping attacks those attacks can be prevented by implementing a good encryption mechanism that will ensure confidentiality of data.

5.3 Network layer – "is also known as transmission layer, is the layer where data from the physical layer are processed and transmitted to the higher-level protocol such as IP, LowPAN, UDP and ICMP"[16]. Furthermore, the network layer is threatened by many attacks, however the countermeasures of this layer will be split into six types, which will be described in sections 5.3.1,5.3.2,5.3.3,5.3.4, 5.3.5 and 5.3.6.

5.3.1 Data Privacy – in term of Network layer to provide data privacy safety control procedures need to the implemented through integrity which will ensure users that are authorized only have access to the system[32]

5.3.2 Security aware ad hoc routing –SAP protocol will prevent attacks from inside the house or close proximity. "The adversary will be dropped from the network after the protocol perform some analysis of the received data[32].

5.3.3 Authentication - good authentication will prevent unauthorized access to the nodes of the IoT devices[32]

5.3.4 Routing Security- implementing routing algorithms will secure the confidentiality of the data.

5.3.5 End-to-end encryption- will provide private communication as the data will be decrypted at the endpoint regardless of how many points it passed through.

5.3.6 GPS tracking system- will track the location of the devices in the Smart Home furthermore, active GPS will be able to detect spoofing attacks.

Network Layer: Security Countermeasures	Implementation Mechanism
Data Privacy	Through Integrity
Security Aware ad hic rotting	SAP protocol
Authentication	Good authentication practices
Routing Security	Implementation of Routing Algorithms
End-To-End Encryption	Implementation of AES 128
GPS	Unable GPS tracking

Table 5: Summary of Network Layer: Countermeasures and Implementation Mechanism

5.4 Data Processing Layer -is the layer in which data is generated and transmitted on the IoT platform. The countermeasures of this layer will be summaries in sections 5.4.1,5.4.2,5.4.3 and 5.4.4.

5.4.1 Web Application Scanner – the use of a web application scanner will help IoT owners to first identify devices that use web applications, second the scanner will help the end-users to evaluate are reduce the risk of threats.

5.4.2 Fragmentation Redundancy Scattering –aims to fragment confidential information to produce fragments that are store in the cloud in this way the risk of data theft is reduced.

5.4.3 Encryption Technique -will ensure data confidentiality, also encryption will prevent against channel attacks.[32]

5.4.4 Hyper Safe – will protect memory pages from being changed, also hyper safe have the option to limited pointing index.[32]

Data Processing Layer: Security Countermeasures	Implementation Mechanism
Web Application Scanner	Vega, WebScarab and Zed attack Proxy
Fragmentation Redundancy scattering	AWS
Encryption technique	RSA
Hyper Safe	Software program

Table 6: Summary of Data Processing Layer: Countermeasures and Implementation Mechanism

5.5 Application layer- allow user to interact with applications on the IoT devices, however the application layer has been described as the weakens link in the IoT platform [16]. Therefore, the countermeasures of the application layer will focus on six areas, which have been included in sections 5.5.1,5.5.2, 5.5.3, 5.5.4, 5.5.5 and 5.5.6.

5.5.1 Data Security -on the application layer could be provided by encryption, authentication, and integrity, if those three measures are applied successfully unauthored access will be prevented and data will be secure[32].

5.5.2 Access Control List (ACLs)- basically allow users to set up a rule on incoming and outgoing traffic and "monitor access request from many users in the IoT system"[32].

5.5.3 Intrusion Detection – is usually implemented through security information and event management systems, where user is alert when unusual action is detected.

5.5.4 Risk Assessment – on the IoT devices in Smart Home can be performed by applying some of the risk assessment frameworks such as OCTAVE Allegro, ISO, NIST and OWASP. Furthermore, the risk assessment will help Smart Home residents to recognize, reduce and mitigate relevant risks.

5.5.5 Firewall – the main aim of the firewall is to prevent unauthorized access to the IoT devices this is done by filtering and block the unwanted packet.

5.5.6 Anti-Virus –the main aim of the anti-virus software is to protect the "confidentiality, reliability and integrity of the IoT network"[32]

Application Layer: Security Countermeasures	Implementation Mechanism
Data Security	Encryption, Authentication, and Integrity
Access Control List	Microsoft's Active Directory ACLs
Intrusion Detection	Anomaly detection in data mining [32]
Risk assessment	OCTAVE, ISO, NIST and OWASP
Firewall	Firewall Software is provided by various vendors
Anti-Virus	Anti-Varus software, Anti-Spyware, and Antiadware is provided by various vendors

Table 7: Summary of Application Layer: Countermeasures and Implementation Mechanism

5.6 Countermeasures: of the Real-World Cases:

5.6.1 Case study 1: Amazon Alexa

In terms of the researcher to be able to identify and summarize Alexa vulnerabilities illustration of how exactly Alexa voice service model work has been illustrated in Table 8 for clarification reasons.

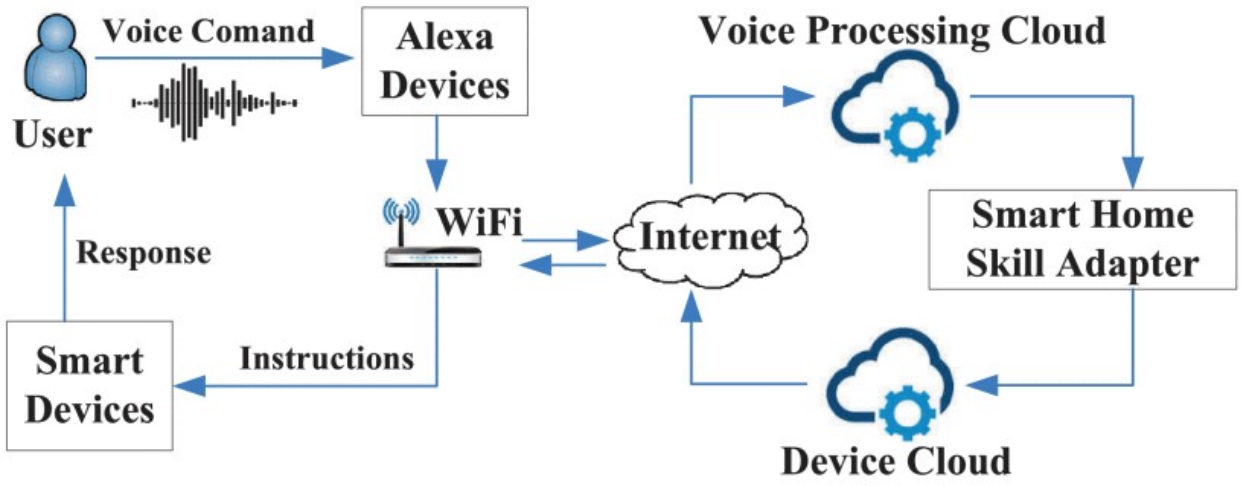

Table 8: Alexa voice service model [33]

Alexa voice service model in Table 8 illustrates how Alexa Control Smart devices in Smart Home Setting. However, the Digital Voice Assistant called Alexa uses only single Factor Authentication based on the voice command, so basically everyone can give a command to your Alexa device without been authenticate. The suitable countermeasure that can be suggested in this scenario is voice that has been biometrically identified, but “voice may vary with ages, illness, or tiredness”[33]Furthermore, user voice is vulnerable to replay attacks is this case wearable device can be introduced to protect Alexa of been hack by replay attack, however wearable devices are not always available to purchase or maybe expensive.

The second main vulnerability Alexa has is Unsecure WI-FI.
Unsecure WI-FI is a very serious threat to any Smart device but when it came to Alexa unsecured WI-FI could be catastrophic because if a malicious party gets unauthorized access to Alexa can use it to hack and control all the other Smart devices in the house. Therefore, to secure the WI-FI in the house, Smart Homeowners need to follow some general advice that experts have suggested in terms of securing the home wireless network. Such as change the router’s administration password, changing the default password is critical because it is “fairly easy for a nearby malicious hacker to access home router”[34] as well as changing wi-fi network password also encryption the wireless network to WPA2 and making sure regular update carried out on the firmware to eliminate any security holes.[34]

Furthermore, researchers have confirmed that Alexa is also vulnerable to the common CrossSite Scripting attack (XSS) in which the hacker has injected malicious code into the browser, however the only countermeasure that can be applied in this scenario is a user awareness

program in which the user needs to educate himself about the potential threat of XSS attacks. Users need to make sure only applications coming from secure sources are installed on the home system in terms to mitigate the risk of XSS attacks.

Amazon Alexa	Step 8: Selecting Mitigation Approach
Single Factor Authentication method	Identify user's voice biometrically
Unsecure Voice Command - replay attacks	Wearable Device
Unsecure wi-fi	Change the router's administration password Change wi-fi network password Encrypt wi-fi wireless network Regularly update router firmware [34]
Cross-Site Scripting	Users should not install unfamiliar applications on the system

Table 9: Summary of Amazon Alexa Vulnerabilities and the Suggested Countermeasures

5.6.1 Case study 2: Samsung Smart Fridge

The main vulnerability of the Samsung Smart Fridge is man -in -the- middle attack due to an invalid SSL certificate. Valid SSL protocol ensures the mitigation to HTTPS.[35] which is encrypted protocol, and a private key is the only one that can establish a valid connection that is associated with the corresponding certificate. Once the valid certificate is installed on the Smart Fridge System Man -In-The Middle attack will not be possible therefore the threat of the Man-In-The-Middle attack will be mitigated.

The second vulnerability of the Samsung Smart Fridge is a botnet attack, as all the IoT devices in the market including the Smart Fridge, come with a default password, limited computation capability and lightweight software. Therefore, the main and most effective way to prevent botnet attacks is to fix firmware by updating, change default settings, create new and unique passwords, make sure the fridge is not running on port 80 HTTP and it is to be changed to HTTPS port 443 simple because HTTP is prone to interception and eavesdropping by attackers[36]. HTTPS port 443 on the other side will offer an encrypted connection using SSL, which will encrypt data when data is sent over the web.

In terms of network security, the network configuration needs to be changed in a way that limits the remote access to IoT devices in the Smart Home, and finally physical hardening of IoT devices in Smart Home can be achieved by storing keys on Trusted Platform modules (TPMS) and Trusted Execution Environment which will ensure "integrity of the disk encryption and password protection platform"[37]

At the end need to be noted that is essential users to act first, instead of hackers because once the IoT devices have been infected, they may be used as a zombie for a very long time and for users will non -technical background will be unnoticeable.

The summarized vulnerability and the prosed countermeasures of those vulnerabilities have been included below in a table.

Samsung Smart Fridge	Step 8 in OCTAVE Allegro: Selecting Mitigation Approach
• Man in the Middle attack due to invalid certificate	• Installed Valid SSL certificate
• DDoS Attacks	• Firmware update to close holes • Change default passwords • Create a new and unique password • Use port 443 on HTTPS • Limit remote access to IoT devices • Hardening the device -store the keys on TPMs and TEE

Table 10: Summary of Vulnerabilities Samsung Smart Fridge and the Suggested Countermeasures

5.6.1 Case study 3: Ring Smart Camera

Ring Smart Camera case has the most diverse set of vulnerabilities of the three cases however, hackers were able to get unauthorized access to the Smart Home system based on two main weaknesses of the Smart Camera the first one no -authentication so anyone can connect to the Smart Camera, the second one bad password hygiene that users of the camera were practicing as the case described earlier the hackers were using already compromised user name and passwords to log in to the camera.

The countermeasure of the Ring Smart camera will advise users to always use two-factor authentication or biometrics, also applied good password hygiene to their IoT devices, as well as always change default passwords, and seek professional and legal advice if needed.

Ring Smart Camera	Step 8 in OCTAVE Allegro: Selecting Mitigation Approach
• Unauthorised access to Smart Home vie your camera	• Change default setting • Change default password • Update the software on the camera regularly • Change the default setting on your router • Make sure the WI-FI connection is secure • Practice good password hygiene
• No authentication	• Use multi-factor authentication • Biometrics
• Non-Compliance with GDPR	• User awareness program • Seek Professional Advice from Information Commissioner Office

Table 11: Summary of Vulnerabilities of Ring Smart Camera and the Suggested Countermeasure

The researcher will not be able to conclude the chapter without proposing a new and improve Smart Home Architecture that will help Smart Homeowner to secure the IoT devices.

5.7 Proposed New Layered IoT Smart Home Architecture

This research project so far has looked at the traditional four-layer IoT architecture that consist of Perception layer, Network Layer, Middleware and Application layer, however the researcher came to the realization that the four-layer architecture is weak architecture, so a new and more secure layered architecture has been proposed that consist of seven layers. Table 12 and Table 13 illustrate the structure of the proposed seven-layered architecture.

Application Layer
Session Layer
Service Layer
Cloud Computing Layer
Network Layer
Fog Computing Layer
Physical Layer

Table 12: Proposed New Layered IoT Architecture

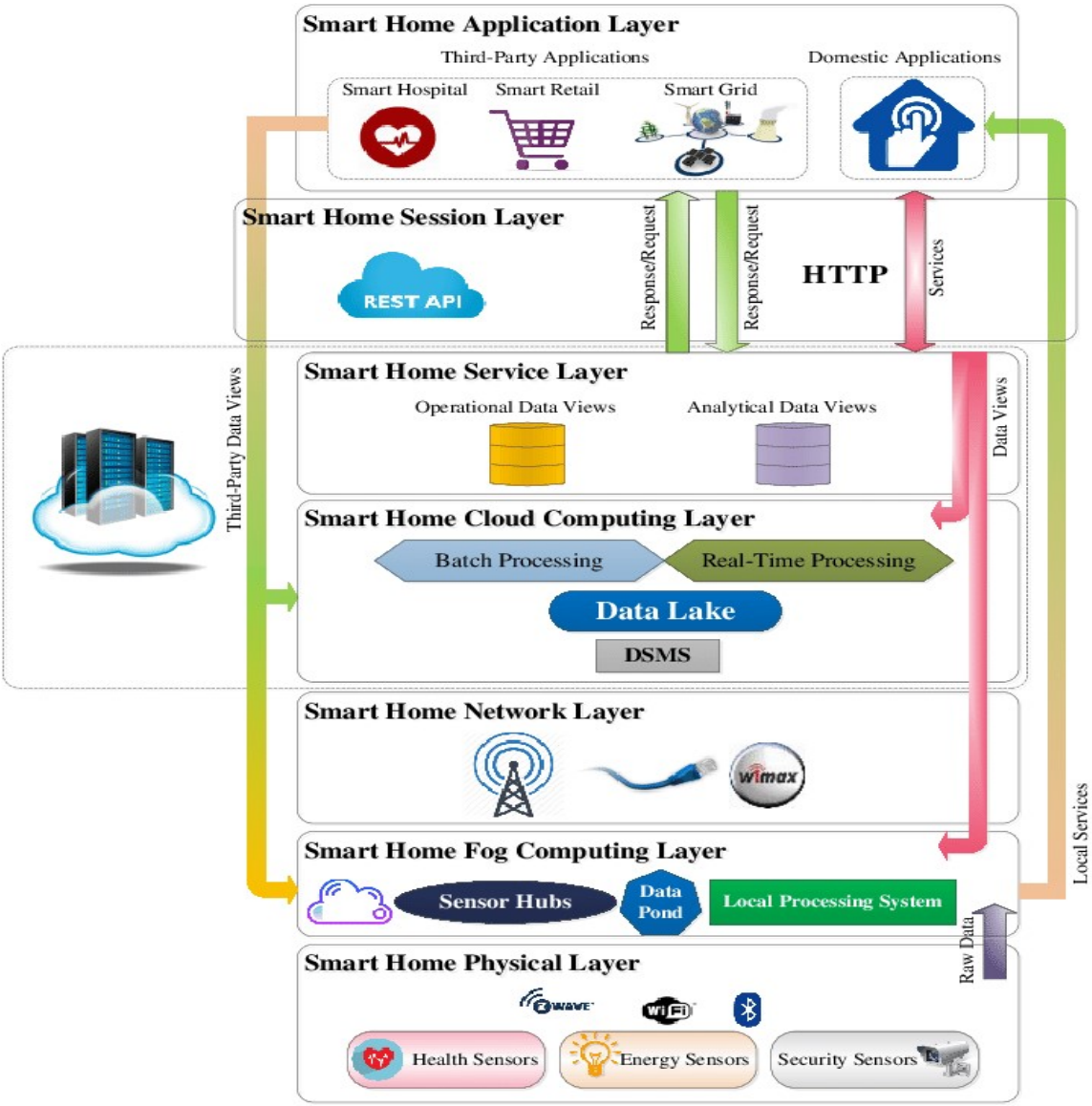

Table 13: Proposed Layer Architecture for Smart Home [38]

The new proposed seven-layer architecture has been designed with security in mind, that will "optimize system performance and deploy security solution for IoT device"[39]
The new proposed architecture has three additional layers: Cloud Computing layer, Fog Computing Layer and Session Computing Layer, each of those layers aims to overcome the security and privacy issues that have been in counted in the traditional four-layer architecture.

The Cloud computing layer has been added to the new architecture design due to the unlimited resources that the cloud can provide to the IoT devices and as experts have identified [12], cloud services are considered to be essentials infrastructure of IoT devices as they "provide support for data storage, data processing and data sharing"[12].However in the most cases, the

cloud computing layer can't operate efficiently enough as is allocated far away from the physical devices, therefore, to overcome the limitations of the cloud. The Fog Computing layer has been added to the proposed architecture. The main purpose of the Fog Computing layer is to fulfill the real-time needs of the IoT devices, such as offloading heavy computational tasks [39] such as encryption.

Overall, the fog and cloud layers collaborate to provide better scalability and flexibility of the system. The fog computing layer also provides better security to the IoT devices as the devices communicate with the fog computing layer first before communicating with the network layer and the cloud computing layer.

The last additional added Layer is the Sessional layer. This layer aims to overcome the energy limitation that some IoT devices In Smart Home are subject to, and due to the limited connection between application and service layer, RESTFUL API and URL – based architecture has been suggested[38]

In conclusion to the new proposed architecture could be concluded that the new architecture aims to provide security solution to the most common cyber security attacks as well as more flexibility and scalability to Smart Home and IoT architecture.

Chapter 6 Conclusion and area of further research

This project has presented the layered architecture of IoT in Smart Home. The reason for that is IoT technologies are the most discussed paradigm today[40]. IoT has the potential to connect all the devices in the world and create a large information system,[40] and significantly improve the life of individuals vie Smart Home, however those great IoT opportunities come with great risks related to cyber and physical attacks.

From the start this study investigate the most common and widely used four-layered architecture and found that the architecture is weak and prone to all types of cyber-attacks, therefore the researcher proposed a new more secure IoT layered architecture to mitigate some of the risks and threats that have been identified in the traditional four-layered architectures.

Furthermore, to make the finding from this project more applicable to real life, three relevant cases studies have been included. Each of those case studies presented a unique set of vulnerabilities to the Smart Home system. Therefore, to mitigate those threats a set of countermeasures has been proposed for each individual case.

Regardless of the case, the main aim of the hacker remains the same, and that is to compromise the confidentiality, integrity, and availability of the IoT Home system.

The next section in this chapter focuses on recommendations and future work of IoT in Smart Home.

6.1 The Project Contributions (Recommendations)

This research has proven the hypotheses that IoT devices are unsecure and prone to many cyber-attacks vie the Internet, this research paper contributes to the field of IoT security by proving suitable countermeasure.

The security of IoT devices in Smart Home lay in the hands of two parties End users and manufactures. End-users need to demand better security of IoT devices as they are the ones that will bear all the negative conveniences of the unsure devices.

This study has investigated and reported some of the consequences that insecure devices could cause and in fact the consequences could be very serious from exposing vulnerable member of the family such as kids to strangers through Ring Camera to having all user personal data exposed to malicious parties as Amazon Alexa case identified.

The consequences of unsecured IoT devices vie Smart Home could last a lifetime, this research has not had the capabilities to describe all the negative consequences that can be inherited from unsecured IoT devices in Smart Home.

This study attempts to suggest that IoT manufactures need to be under the obligation to produce devices that have been tested for common cyber-attacks, the security of IoT devices needs to be seen as a compulsory requirement not an optional choice of the manufacture. In this way some of the most common cyber-attacks that IoT devices had experienced could be avoided.

6.2 Limitations and Future Work

Despite all the negatives, the future of IoT vies Smart Home is bright manufactures and endusers needs to be able to collaborate and work together to achieve innovation and security in Smart Home. A worldwide standard and a recognized framework need to be developed to overcome the existing threats and vulnerabilities.

This study paper comes with its limitations the biggest limitation that this project has in counted is the complexity and diversity of smart devices, the lack of standards and the limited support to end users vie the manufactures.

Bibliography /References

[1] M. Li, W. Gu, W. Chen, Y. He, Y. Wu, and Y. Zhang, "ScienceDirect ScienceDirect Smart Home : Architecture, Technologies and Systems," *Procedia Computer Science*, vol. 131, pp. 393–400, 2018, doi: 10.1016/j.procs.2018.04.219.

[2] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors (Switzerland)*, vol. 18, no. 3, Mar. 2018, doi: 10.3390/s18030817.

[3] P. Dorey, "Securing the internet of things," in *Smart Cards, Tokens, Security and Applications: Second Edition*, Springer International Publishing, 2017, pp. 445–468. doi: 10.1007/978-3-319-50500-8_16.

[4] A. D. Jurcut, P. Ranaweera, and L. Xu, " Introduction to IoT Security ," *IoT Security*, pp. 27–64, Feb. 2020, doi: 10.1002/9781119527978.CH2.

[5] "Standards for Cybersecure IoT Devices: A Way Forward - Centre for International Governance Innovation."

https://www.cigionline.org/publications/standardscybersecure-iot-devices-way-forward/ (accessed Jun. 03, 2021).

[6] "Saunders, Lewis & Thornhill, Research Methods for Business Students, 7th Edition | Pearson." https://www.pearson.com/uk/educators/higher-educationeducators/program/Saunders-Research-Methods-for-Business-Students-7thEdition/PGM1089011.html (accessed Jun. 03, 2021).

[7] "(PDF) Robert K. Yin. (2014). Case Study Research Design and Methods (5th ed.). Thousand Oaks, CA: Sage. 282 pages." https://www.researchgate.net/publication/308385754_Robert_K_Yin_2014_Case_Study_Research_Design_and_Methods_5th_ed_Thousand_Oaks_CA_Sage_282_pages (accessed Jun. 03, 2021).

[8] "Inside the Smart Home - Google Books." https://www.google.co.uk/books/edition/Inside_the_Smart_Home/3J0MBwAAQBAJ?hl=en&gbpv=1&pg=PA1&printsec=frontcover (accessed Jun. 03, 2021).

[9] R. Zaheer and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," pp. 257–260, 2012, doi: 10.1109/FIT.2012.53.

[10] "IoT Technology and Smart Devices in the Home | Clutch.co." https://clutch.co/developers/internet-of-things/resources/iot-technology-smartdevices-home (accessed Jun. 03, 2021).

[11] I. K. K. N. I. N.-F. G. S. G. Balini. D.Geneiatakis, "Security and privacy issues for an IoT based home," *International Convention on Information and Communication Technology, Electronics and Microelectronics,* , pp. 1292–1297, 2017.

[12] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering*, vol. 2017. Hindawi Publishing Corporation, 2017. doi: 10.1155/2017/9324035.

[13] T. Publication, "INTERNET OF THINGS: A REVIEW ON ARCHITECTURE, SECURITY THREATS AND COUNTERMEASURES", [Online]. Available: https://www.academia.edu/37418771/INTERNET_OF_THINGS_A_REVIEW_ON_ARCHITECTURE_SECURITY_THREATS_AND_COUNTERMEASURES

[14] M. Aydos, Y. Vural, and A. Tekerek, "Assessing risks and threats with layered approach to Internet of Things security," *Measurement and Control (United Kingdom)*, vol. 52, no. 5–6, pp. 338–353, Jun. 2019, doi: 10.1177/0020294019837991.

[15] M. Aydos, Y. Vural, and A. Tekerek, "Assessing risks and threats with layered approach to Internet of Things security," *Measurement and Control (United Kingdom)*, vol. 52, no. 5–6, pp. 338–353, Jun. 2019, doi: 10.1177/0020294019837991.

[16] "(PDF) On the Performance Analysis of Optical Wireless Communication Systems." https://www.researchgate.net/publication/343239565_On_the_Performance_Analysis_of_Optical_Wireless_Communication_Systems/figures?lo=1&utm_source=google&utm_medium=organic (accessed Jul. 20, 2021).

[17] M. Aydos, Y. Vural, and A. Tekerek, “Assessing risks and threats with layered approach to Internet of Things security,” *Measurement and Control*, vol. 52, no. 5–6, pp. 338–353, 2019, doi: 10.1177/0020294019837991.

[18] Heartfield Ryan and Gan Diane, “(PDF) Social Engineering in the Internet of Everything.” https://www.researchgate.net/publication/305495988_Social_Engineering_in_the_Internet_of_Everything/figures (accessed Jun. 10, 2021).

[19] “Detecting DoS Attack in Smart Home IoT Devices.” https://rpaudel42.github.io/pages/iot.html (accessed Jun. 18, 2021).

[20] “risk definition nist - Google Search.” https://www.google.com/search?q=risk+definition+nist&oq=risk+definition&aqs=chrome.0.35i39j69i57j0i67j0l7.3615j1j7&sourceid=chrome&ie=UTF-8 (accessed Jun. 16, 2021).

[21] “Comparison between MONARC and different Risk Management Methods - MONARC.” https://www.monarc.lu/publications/comparison-between-monarcand-different-risk-management-methods/ (accessed Jun. 18, 2021).

[22] “Alexa, Google Assistant, and Apple HomeKit: Your Guide to Smart Home Ecosystem Options.” https://www.iotforall.com/comparing-smart-home-ecosystemoptions-alexa-google-assistant-apple-homekit (accessed Jun. 23, 2021).

[23] “Amazon Alexa - Wikipedia.” https://en.wikipedia.org/wiki/Amazon_Alexa (accessed Jun. 23, 2021).

[24] “• Amazon Echo global shipments 2014-2025 | Statista.” https://www.statista.com/statistics/1022701/worldwide-amazon-echo-unitshipment/ (accessed Jun. 23, 2021).

[25] “Why You Must Beware What You Ask Amazon Alexa.” https://www.forbes.com/sites/zakdoffman/2020/08/13/amazon-alexa-cyber-attackcheck-point-report-smart-speaker-warning/?sh=5d5e59d35008 (accessed Jun. 23, 2021).

[26] “Smart refrigerator hack exposes Gmail account credentials | Network World.” https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposesgmail-login-credentials.html (accessed Jul. 27, 2021).

[27] “Ring Stick Up Cam Battery by Amazon | HD security camera with Two-Way Talk, Works with Alexa | With 30-day free trial of Ring Protect Plan | White : Amazon.co.uk: Amazon Devices & Accessories.” https://www.amazon.co.uk/ringstick-up-cam-battery-hd-security-camera-with-two-way-talk-works-withalexa/dp/B07Q4R7VWN/ref=asc_df_B07Q4R7VWN/?tag=googshopuk21&linkCode=df0&hvadid=375463890634&hvpos=&hvnetw=g&hvrand=12224315874430599416&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1007091&hvtargid=pla-830684917649&psc=1&tag=&ref=&adgrpid=85278568948&hvpone=&hvptwo=&hvadid=375463890634&hvpos=&hvnetw=g&hvrand=12224315874430599416&h

vqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1007091&hvtargid=pla8306 84917649 (accessed Jul. 28, 2021).

[28] "Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs | Amazon | The Guardian." https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hacklawsuit-threats (accessed Jul. 28, 2021).

[29] "How to stop hackers from spying on you through your Amazon Ring security camera or doorbell - Deseret News." https://www.deseret.com/indepth/2020/1/3/21043653/amazon-ring-hacking-casesdoorbell-santa-claus-kids-bedroom-safe-lawsuit-security-camera-home-hacker (accessed Jul. 28, 2021).

[30] "Experts find Amazon Alexa bug that lets hackers control device | Daily Mail Online." https://www.dailymail.co.uk/sciencetech/article-8628419/Securityexperts-major-vulnerabilities-Amazon-Alexa-lets-hackers-control-device.html (accessed Jun. 28, 2021).

[31] A. Wahab Ahmed, M. Muhammad Ahmed, O. Ahmad Khan, and M. Ali Shah, "A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT," 2017. Accessed: Jun. 14, 2021. [Online]. Available: www.ijacsa.thesai.org

[32] "IEEE Xplore Full-Text PDF:" https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8433167 (accessed Jul. 07, 2021).

[33] "10 Ways to Strengthen Alexa Privacy and Security - dummies." https://www.dummies.com/consumer-electronics/smart-devices/10-ways-tostrengthen-alexa-privacy-and-security/ (accessed Jul. 14, 2021).

[34] "SSL Certificates vs. Man-in-the-middle attacks | by Roman Munteanu | Medium." https://medium.com/@munteanu210/ssl-certificates-vs-man-in-the-middle-attacks3fb7846fa5db (accessed Jul. 29, 2021).

[35] C. Kelly, N. Pitropakis, S. McKeown, and C. Lambrinoudakis, "Testing and Hardening IoT Devices against the Mirai Botnet," Jun. 2020. doi: 10.1109/CyberSecurity49315.2020.9138887.

[36] "(1) New Message!" https://www.keyfactor.com/blog/top-10-iot-vulnerabilities-inyour-devices/ (accessed Jul. 07, 2021).

[37] "IEEE Xplore Full-Text PDF:" https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8629861 (accessed Jul. 17, 2021).

[38] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 195–202, May 2020, doi: 10.1016/J.DCAN.2019.08.006.

[39] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," *Applied Sciences 2020, Vol. 10, Page 4102*, vol. 10, no. 12, p. 4102, Jun. 2020, doi: 10.3390/APP10124102.

[40] “(PDF) Introduction to IoT Security.” https://www.researchgate.net/publication/336406296_Introduction_to_IoT_Security (accessed Jul. 22, 2021).