Real-Time Internet of Things Security

(RIoTS)

By

Eman Fatima

Asifa Iqbal

Shaheer Ahmad

M Mustafa Zahoor

Project Supervisor: Asst. Prof. Waleed Bin Shahid

Submitted to the faculty of Department of Electrical Engineering,
Military College of Signals, National University of Sciences and Technology, Islamabad,
in partial fulfillment for the requirements of B.E Degree in Electrical (Telecom) Engineering.

June 2022

In the name of ALLAH, the Most benevolent, the Most Courteous

CERTIFICATE OF CORRECTNESS AND APPROVAL

This is to officially state that the thesis work contained in this report

"Real-Time Internet of Things Security"

is carried out by

Eman Fatima, Asifa Iqbal, Shaheer Ahmad and M Mustafa Zahoor

under my supervision and that in my judgement, it is fully ample, in scope and excellence, for the degree of Bachelor of Electrical (Telecom.) Engineering in Military College of Signals, National University of Sciences and Technology (NUST), Islamabad.

Approved by

Supervisor
Asst. Prof. Waleed Bin Shahid
Department of IS, MCS

Date: _____

DECLARATION OF ORIGINALITY

We hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification in either this institute or anywhere else.

ACKNOWLEDGEMENTS

Allah Subhan'Wa'Tala is the sole guidance in all domains.

Our parents, colleagues and most of all supervisor, Asst. Prof. Waleed Bin Shahid without your guidance.

The group members, who through all adversities worked steadfastly.

Plagiarism Certificate (Turnitin Report)

This thesis has 13% similarity index. Turnitin report endorsed by Supervisor is attached.

_____

Eman Fatima

00000261278

_____

Asifa Iqbal

00000284103

_____

Shaheer Ahmad

00000278791

_____

M Mustafa Zahoor

00000249296

_____

Signature of Supervisor

Abstract

The field of Internet of things and worldwide real time information exchange is gradually increasing. IoT devices and services are becoming more widely available. Threats and assaults against IoT devices and services are also on the rise as a result of their success. In the IoT world, cyber-attacks are nothing new, but as the IoT gets more deeply embedded in our lives and communities, it will be critical to step up and take cyber defense seriously.

Our project aims to safeguard everyday IoT devices being used by society. RIoTS will be installed at the gateway, allowing all data exchanged and created by smart IoT devices to pass through. Using pre-trained machine learning algorithms, it would be able to detect unusual entrance and egress traffic, as well as cyber-attacks like analyzing what information goes out of the network, and it captures the traffic and analysis that, sees if there are weak passwords that can be compromised, it checks whether devices are vulnerable to DoS attacks, whether remote code can be executed over them, whether the communication they are using with the rest of the internet is unencrypted or not, if information is being leaked and whether there are configuration issues that the attacker can exploit because even one of these internal IoT device is compromised then it will act as a pivot point to launch wider range of attacks on rest of the IoT network. By securing smart IoT devices, RIoTS can help assure data privacy and security.

Keywords: Internet of things, real time information, data privacy and security, Cyber-attacks.

Table of Contents

List of Figures

CHAPTER 1: INTRODUCTION

CHAPTER 01

INTRODUCTION

1.1. Chapter Overview

This chapter sketches a detailed introduction of RIoTS, accentuating the problem statement, objectives, scope and reason for the exception of the project under discussion.

1.2. Problem statement

The Internet of Things (IoT) is a network of physical objects with embedded electronics that can communicate and sense interactions with one another and the outside environment. In the coming years, IoT-based technology will provide improved levels of service, effectively transforming how people live their lives. Medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a few of the fields where IoT has made a significant impact.

As the technology is evolving every day, people are relying more on the advanced smart devices such as smart watch, smart camera, baby monitors and multiple devices which are used in our daily lives. Little do they know that with increasing demand of these devices, the security considerations are overlooked and vulnerable IoT devices are being designed. This opens the door for adversaries, which often exploit such devices with little or no effort. Attacker can easily find the flaws and compromise the security of such devices. By compromising, the attacker gets a hold of the device and access to the

information stored on it. The information can be exploited by any means and thus is a great threat.

Security managers are focused on preventing network and web attacks by preventing all types of penetration, but nothing is done to identify and mitigate the attacks in a single solution. By combining identification and mitigation, our project bridges this distance. With the number of attackers and the sophistication of their DoS, Scanning, and Web attacks rapidly increasing, it is more important than ever to monitor and record their activities and collect information that can help improve existing security tools.

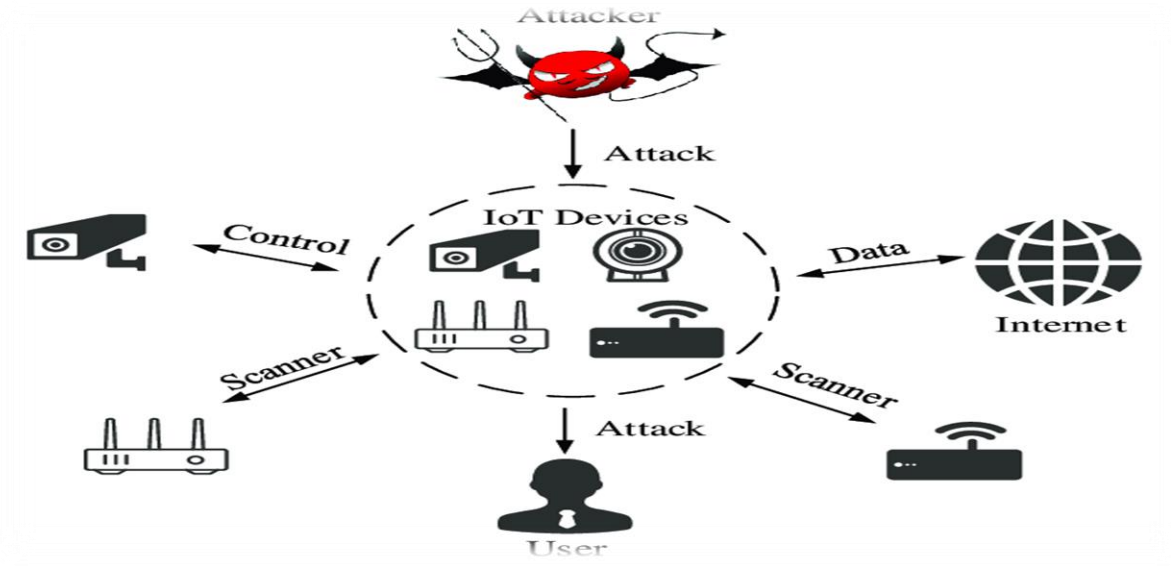

Figure 1-1 IoT Devices

1.3. Objectives

- **Creation of a minor IoT system**

An Internet of Things platform connects device sensors to data networks. It gives you access to the data that the backend application uses. An IoT platform enables developers to disperse apps, collect data remotely, secure connectivity, and monitor sensors. We intend to develop a limited IoT network consisting of the necessary components, interconnecting nodes and smart device(s) for being able to complete necessary tasks required of an IoT system.

- **Launching a number of attacks on said system**

  Internet of things (IoT) connects devices remotely with the easy operability. Because of particular aspects of the underlying technology, threats against IoT systems and devices translate to higher security risks. With an IoT system in actuation we intend to launch cyber-attacks on said system to compromise normal functionality

  Some common cyber-attack types are enlisted:

  1. Physical attacks: This sort of attack tampers with hardware components. The majority of gadgets are used in locations where they are vulnerable to physical attacks.

  2. Reconnaissance attacks: unauthorized discovery of service, or vulnerability detection and mapping. Scanning network ports, packet sniffers, traffic analysis, and making queries regarding

IP address information are all examples of reconnaissance attacks.

3. Denial-of-service (DoS): This kind of attack is an attempts to make a machine or network resource unavailable to its intended users. The majority of IoT devices are vulnerable to this attack because of low memory capabilities and limited computation resources

4. Access attacks – unauthorized persons gain access to networks or devices to which they have no right to access. There are two types of access attack: physical access, whereby the intruder can gain access to a physical device. The second is remote access, where an intruder can remotely access internet-connected devices.

5. Attacks on privacy: Because enormous amounts of data are easily accessible through remote access mechanisms, privacy protection in IoT has become increasingly challenging.

- **Detection and remedial measures after analysis of attacks**: Proposing an attack detection model for protection of IoT/smart devices from such attacks

1.4. Justification for the Selection of Topic

The absence of a system that detects and mitigates attacks on an IoT device motivated us to create our handy device, which is easy to use, carry, configure and upgrade. Moreover, the proposed solution can easily be merged with any existing security solution and is not costly. It would not share any user data with the vendor, making it trustworthy and easily adaptable.

1.5. Scope

To establish an indigenous secure anonymous network for Pakistan on a relatively smaller scale that makes use of

- Hardware – Raspberry Pi 3.0 (with LCD Display)
- Software

– Windows 10

– PyCharm 2018.2.2

– Raspbian

– Linux

– Ubuntu

- Networks – Socket programming, TCP/IP – Threading/ Multi-threadin

This project might be used in various disciplines like e-commerce, sensitive organizations, the healthcare sector, and the entire security sector of the country since it allows for the identification and prevention of attacks in real-time. It can reduce compromised privacy in banks and secure other confidential information, such as stocks and client personal data, in several multinational corporations and offices.

The project's primary purpose is to supplement and incorporate existing security tools while also providing resistance to attacker evasion. As a result, we hope to use this project to combine our theoretical expertise with practical experiences to improve our network security. This project aims to create a complete security solution with its machine learning detection system and a raspberry gateway to analyze attacks.

1.6. Contributions

This project was created primarily to protect networks against DoS, Scanning, and Web attacks by real-time identification and mitigation of said attacks. Providing insight into the attackers' activities and allowing researchers to understand the attackers' strategies better. As a result, they can integrate and improve the existing architecture.

1.7. Chapter Summary

The current chapter elucidates a comprehensive overview of the project under discussion, thus explaining the introductory details, including scope, problem definition and reason for selecting the project RIoTS.

CHAPTER 2: LITERATURE REVIEW

CHAPTER 02

LITERATURE REVIEW

2.1. Overview

This chapter deals with comprehensive details of attacks on IoT devices and solutions offered worldwide, their limitations and the uniqueness of our proposed solution.

2.2. Project Domain

As the world progresses towards automation and smart cities in the internet age, nearly everyone is connected to the internet via Wi-Fi Access points. Smart IoT devices are now everywhere. They make our life easier by conversing, sharing information, and doing vital tasks.. As devices are easy to use, their increasing demand lessened the focus on securing devices. This leads to privacy and security concerns for businesses, governments and smart cities. The necessity to defend these smart devices from cyber-attacks is critical.

2.3. Background

Advancements in digital communication, leading to increased security and privacy concerns, have urged researchers to develop different tools and solutions so far. A secure IoT device has always been required to preserve the communication among local wifi networks. Usually, a raspberry gateway is used to serve the need. Still, the problem lies in the fact that smart devices provide extensive anonymity but cannot encrypt the data for

the users. On the contrary, RIoTS successfully secure real-time information but does not hide the identities of communicating parties. For IoT devices, the best solution up to date provides both security and anonymity. Still, it is slack, prohibited in some countries and cannot be availed by intelligence agencies and the Pak military because of surveillance and scrutiny. The elucidation of these problems resides in an endemic network that can provide complete security and anonymity to the web traffic.

2.4. Literature Review

With billions of IoT devices, applications, and services currently in use and more on the way, it's clear that the Internet of Things is here to stay. For very same reason, IoT security is paramount. Cyberattacks can be launched using poorly secured IoT devices and services, compromising sensitive data and endangering individual users' safety. This literature review aims to gain an understanding relevant to our project, Real-Time Internet of Things Security.

2.4.1. Threat modelling of Smart Light Bulb

The first paper which we studied is Threat modelling of Smart Light Bulb. In this paper, the author mainly focuses on the security and possible attacks related to CoAP and Zigbee protocols, and the method used to identify threats is the threat model. The AD Tool (Attack-Defense trees) is chosen to model the threats. The attacks mentioned in this paper are Worm attacks, Hacking Smart Light bulbs using Bluetooth, and DDoS attacks called Botnet.

2.4.2. Smart bulb using IoT

The second paper studied is the smart bulb using IoT. It can be controlled by using the internet. In this paper, a smart battery charger is designed to continuously provide a power supply to the bulb without any stop. This project combines a solar power inverter, a wireless power transfer idea for power generation, and a home automation system based on the Internet of Things (IoT).

2.4.3. Taxonomy of Security Attacks

The third paper studied is Taxonomy of Security Attacks. In this paper, there are several types of attacks on IoT, such as Spoofing/Altering/Replay Routing attacks, Denial of Service (DoS) attacks, Sybil attacks, and node capture attacks in IoT. There are some limitations mentioned in this research paper, like it outlines the various attacks on appropriate security measures.

2.5. Research Based Results

2.5.1. IP Camera

A case study of a web IP camera will discover the existing security models in the camera and try to find out the further vulnerabilities of this IP camera. In smart cities or smart homes, all the devices connected via the internet face the maximum threat problems. Web IP camera is employed outside buildings and homes for protection. It can be monitored through android phones.

Figure 2-1 IP Camera

2.5.1.1. Security Analysis

Three security flaws were found while studying IP camera.

- First it is not using secure channel for communication, all sensitive data was transferred in clear text without using any encryption techniques.
- Second is RTSP URL used to stream data was brute forcible as it a common RTSP URL.
- Third is IP camera account credentials are stored in clear text and not encrypted within the mobile application.

Any attacker can get access to the camera provided that the camera is connected to the internet and gets video information just by having its IP address. Attackers can even scan the internet to find open RTSP ports and try common URLs which this camera uses to broadcast its video information.

2.5.2. Nest Thermostat

Nest Thermostat is a smart device that uses learned behaviour to manage air conditioning (HVAC) units. The thermostat has a motion..sensor that detects whether users are present at the installed site, as well as a WiFi module that allows it to connect to the user's home or business network and interact with the Nest Cloud, allowing it to be controlled remotely. It also has a ZigBee..module that allows it to communicate with other Nest devices

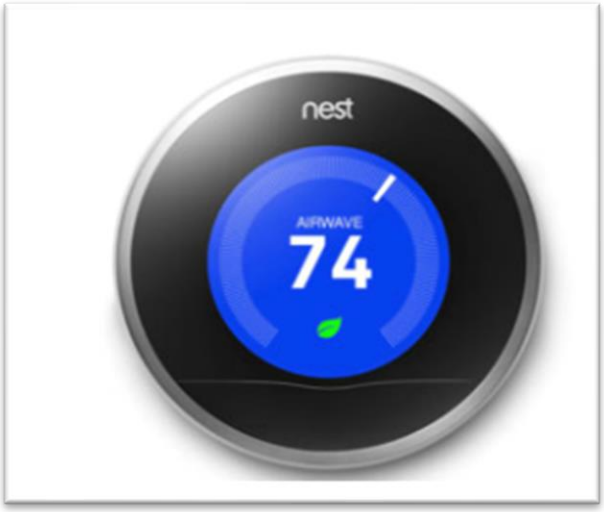

Figure 2-2 Nest Thermostat

Steps taken to compromise the device:

- Setting system _boot [5] pin to be pulled high.
- Trojan Injection.
- Custom Kernel generation with debugging capabilities.

2.5.3. Nike Fuelband

The Nike comes with a normal USB port that may be used to charge and sync your device. This connector can also be used to update the device's firmware, although it does not offer external access to the BOOT0 pin. As such, the device must be opened. The fact that the microcontroller is built as a Ball Grid Array (BGA) further complicates the situation, as there is no direct access to the BOOT0.

Figure 2-3 Nike Feulband

External reads and writes are locked against the internal flash by the microprocessor, effectively isolating the device's firmware from the outside

world. This protection was not employed on Nike. As a result, an attacker with physical access to the device can freely modify the contents of flash.

2.5.3.1. Vulnerabilities

The circuit board's traces must then be followed in order to come across a test point that indirectly exposes the pin in issue. Following this procedure, we were able to detect the BOOT0 pin indirectly, which was then driven to logic 1 using a 100 V resistor linked to..VDD. This allowed us to gain access to the alternate..boot mechanism and take advantage of the device's lack of read/write security. Using standard ST Microelectronics development tools, communication..over USB with the STM32.was achieved, and the device’s firmware..was obtained. We began modifying the device's firmware once we had it in our hands.

2.5.3.2. Firmware Testing

The most basic alteration is a string replacement, which involves locating a string in the program that is displayed at some time and replacing it with something different. After making the update, the device's modified firmware was written to it, only to discover that normal functioning had vanished. Further testing revealed that the failure to compute the right CRC for the image was to blame. The check failed because the image had been altered.

2.5.3.3. Results

A closer look into the disassembled firmware image revealed that it used the STM32 microcontroller's CRC engine to validate its authenticity by comparing the result of the checksum. CRC computation against a stored value. This value could be changed because it was located within the image. The patched firmware was delivered to the device and verified to work after adding the necessary checksum.Boot0 pin not accessible.

- Select a different boot mechanism.
- Take advantage of the device's lack of read and write protection.Communication over USB was achieved.
- The device’s firmware was obtained.
- String replacement.
- The disassembled firmware image.
- This value was found within the image itself.

2.6. Conjecture

Since all the above-mentioned anonymity solutions have stated issues and complications which have made them unreliable and risky, thus urging the need of an effective and innovative solution that will corroborate the provision of utter anonymity and security, thus promising the internet users with the solution of all their reservations..regarding cyber threats and cyber vulnerabilities.

2.7. Chapter Summary

The above chapter incorporated the details of different tools used today in order to attain security. It comprised of comprehensive study of smart devices and the issues that occur at the cost of their employment. It also includes the concerns addressed by the different companies.

CHAPTER 3:

TECHNICAL SPECIFICATIONS

CHAPTER 03

TECHNICAL SPECIFICATION

3.1. Overview

This chapter covers the project's technical requirements as well as the specifics of the project's key steps as it progresses.

3.2. Network Diagram

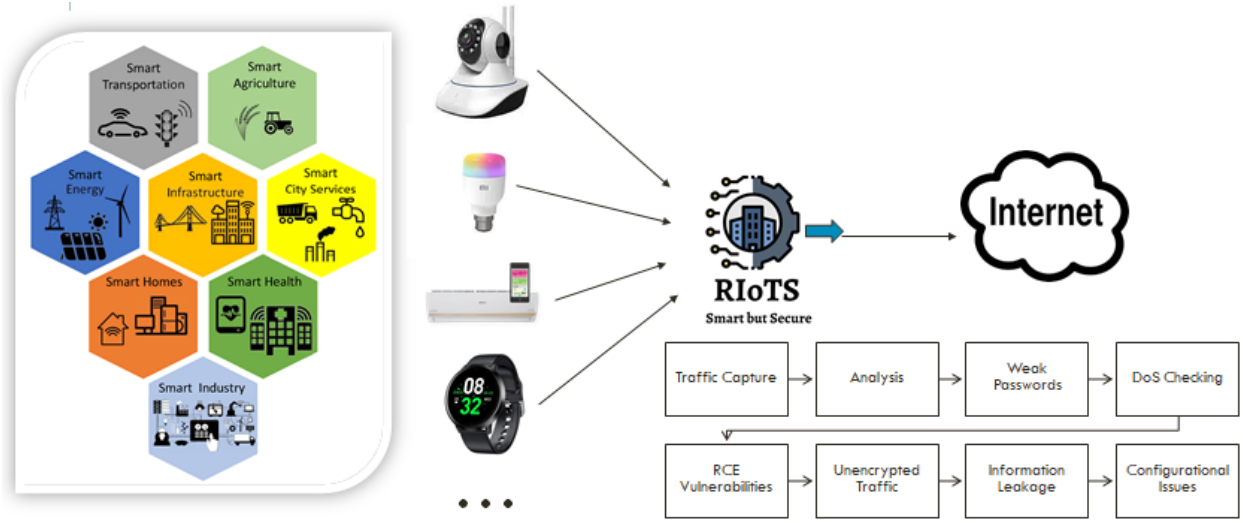

Figure 3-1 RIoTS

RIoTS would work as depicted in the network diagram above. In a general environment IoT devices communicate with their routers gateway towards the internet. These devices

are communicating valuable & critical user data without check, hence inviting attackers to take advantage of this fact

So RIoTS works in a way that it ensures real-time IoT security, the solution essentially sits behind these devices and the network gateway in order to analyze the information goes out of the network, and how it captures the traffic and analyses that, sees if there are weak passwords that can be compromised, it checks whether devices are vulnerable to DoS attacks, whether remote code can be executed over them, whether the communication their using with the rest of the internet is unencrypted or not, if information is being leaked and whether there are configuration issues that the attacker can exploit because even one of these internal IoT device is compromised then it will act as a pivot point to launch wider range of attacks on rest of the IoT network.

3.3. Methodology

Our solution can basically be broken down into three stages. First would consist of the procurement of IoT based hardware which would be in-use in society and would a great threat if compromised. Second would be to devise ways of compromising these devices in order to bring forward their flaws and eventually shut them down. Lastly to produce ways to counter the security flaws found before and implement them in real-time.

In this chapter, we will discuss first stage that is hardware procurement. Rest two stages will be discussed in further chapters

3.4. Stage 1: Hardware Procurement

3.4.1 Xiaomi Smart Bulb

Figure 3-2 Xiaomi Smart Bulb

Specifications:

- Service Life:Approx.25,000 h
- On/off：125000 Cycles
- Operating Temperature:-10°C to 40°C
- Operating Humidity:0–85% RH
- Operating Frequency:2412–2472 MHz

- Maximum Output Power:17.41 dBm

3.4.2 IP Smart Camera

Figure 3-3 IP Smart Camera

Specifications:

• Brand	V380
• Shape	Dome(Indoor)
• Camera Resolution	2 MP

• Camera Technology	Network/IP/Wireless
• Camera Range	10 to 20 m
• Max. Image Resolution	1280 x 720
• Minimum Order Quantity	5

3.4.3 Raspberry Pi

The last hardware utilized in the project is Raspberry Pi 3.0. It is a portable and rechargeable device which is password protected. This module performs all the necessary processing required for security of IoT device. It will act as a gateway to the devices and detect the attacks in real time. Raspberry Pi is also responsible for the filtration of malicious URLs. Raspberry Pi 3 is basically a development aboard in PI series. It can be contemplated as a solitary board computer which works on Linux OS. The board, in addition of having several characteristics, also has a tremendous processing speed, making it appropriate for modern applications. The Raspberry Pi hardware has advanced through numerous versions which highlight distinctions in peripheral-device provision and memory capacity.

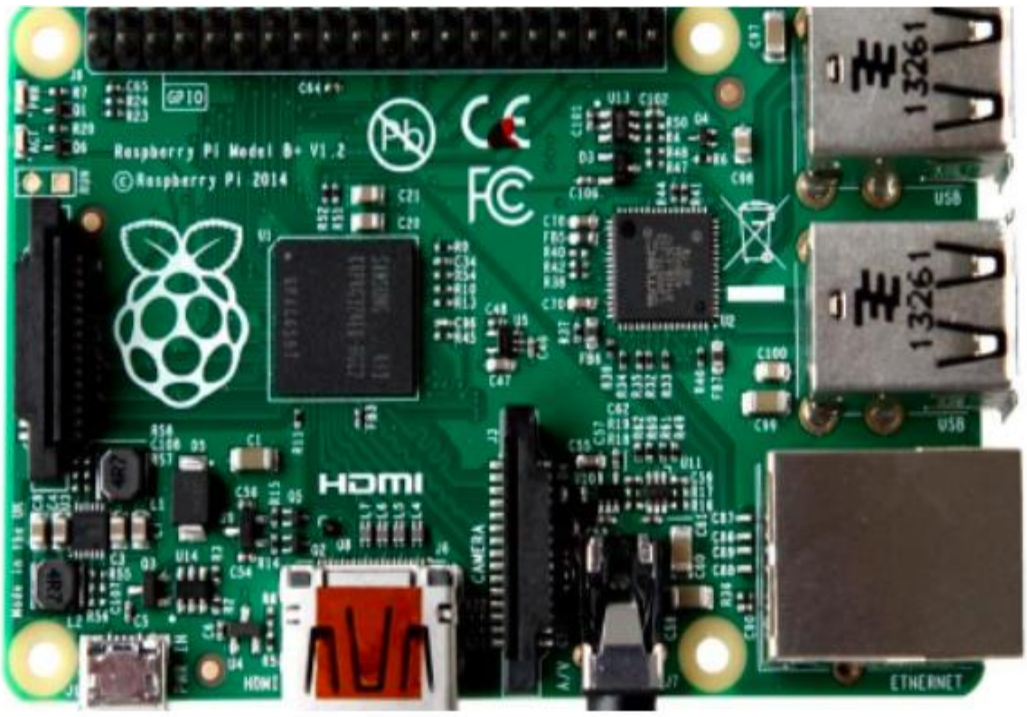

Figure 3-4 Raspberry pi

3.5. Chapter Summary

This chapter gives insight to the methodology used for the project. It gives the description and specifications of hardware devices used in our project.

CHAPTER 4: PROPOSED SOLUTION

CHAPTER 04

PROPOSED SOLUTION

4.1 Chapter Overview

The following chapter explicates the entire technical working of the project under discussion, including launching of attacks and its countermeasures part. It describes the modes in which the solution operates and tells about the problems which RIoTS resolved.

4.2 Stage 2: Launching Attacks

Now we will discuss in detail the attacks launched on our procured devices.

4.2.1 Xiaomi Smart Bulb:

4.2.1.1 ARP Poisoning:

We start by starting up the Ettercap tool in Kali Linux, which we will use to perform a man-in-the-middle attack on the Smart bulb. Ettercap is an all-in-one solution for man-in-the-middle attacks. It has live connection sniffing, on-the-fly content filtering, and many other cool features. It provides various network and host analysis functions, as well as active and passive protocol dissection.

Figure 4-1Ettercap Interface

- Connect to the network that the smart bulb is on and click on ‘scan for hosts’ from the drop-down menu. A search will pop up and automatically search for all available hosts on the connected network

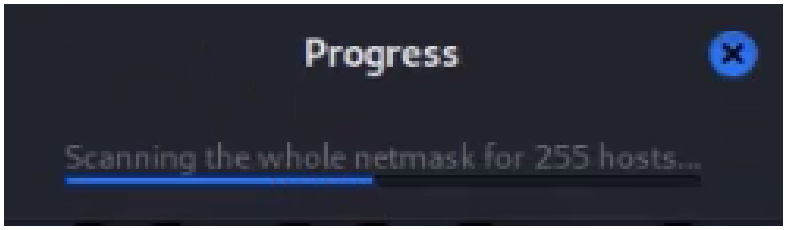

Figure 4-2 Search for hosts

- All the scanned hosts can be viewed by clicking on ‘show hosts’ from the drop-down menu. All hosts will be displayed with their IP addresses and MAC addresses.

Figure 1-3 List of available hosts

- Add the smart bulb as target 1 by manually searching for its IP address from the list.

- Add the router as target 2 by manually searching for the gateway IP from the list.

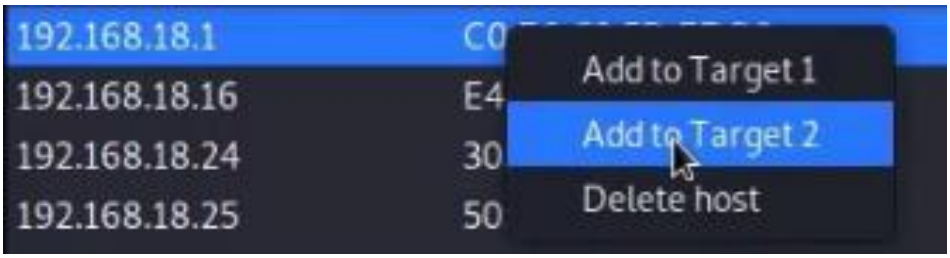

Figure 4-4 Adding devices as targets

Begin ARP poisoning by selecting it from the drop-down menu. ARP poisoning is successful, and your device will be the man-in-the-middle between the smart bulb and the router.

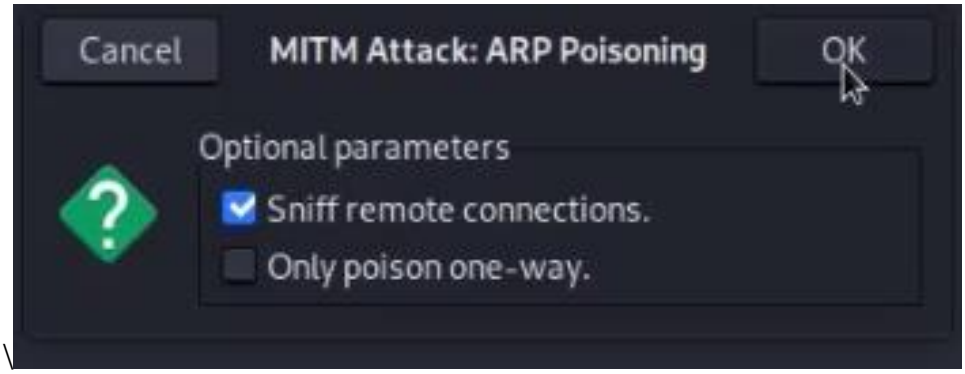

Figure 4-5ARP poisoning

4.2.1.2. Traffic Analysis

Startup Wireshark tool in Kali Linux and select the option with an active internet connection. Wireshark is the world's most popular and widely used network protocol analyzer. It is the de facto (and frequently de jure) standard across many commercial and non-profit organisations, government agencies, and educational institutions because it allows you to observe what is occurring on your network at a microscopic level. The development of Wireshark is still going strong because to voluntary contributions from networking experts all over the world, and it is a continuation of Gerald..Combs' 1998 effort.

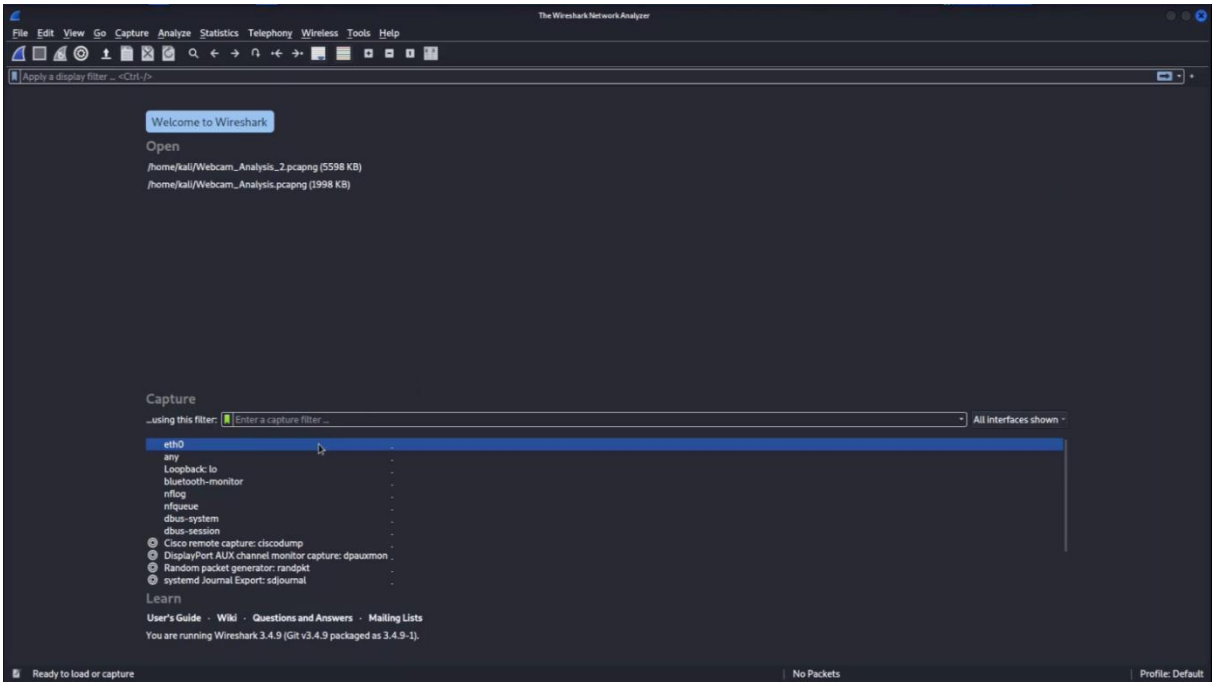

Figure 4-6 Wireshark interface in linux

Now all the communication between the smart bulb and the router will pass through your device. Enter the IP address of the smart bulb in the filter available above so only the relevant communication is displayed and is visible for analysis.

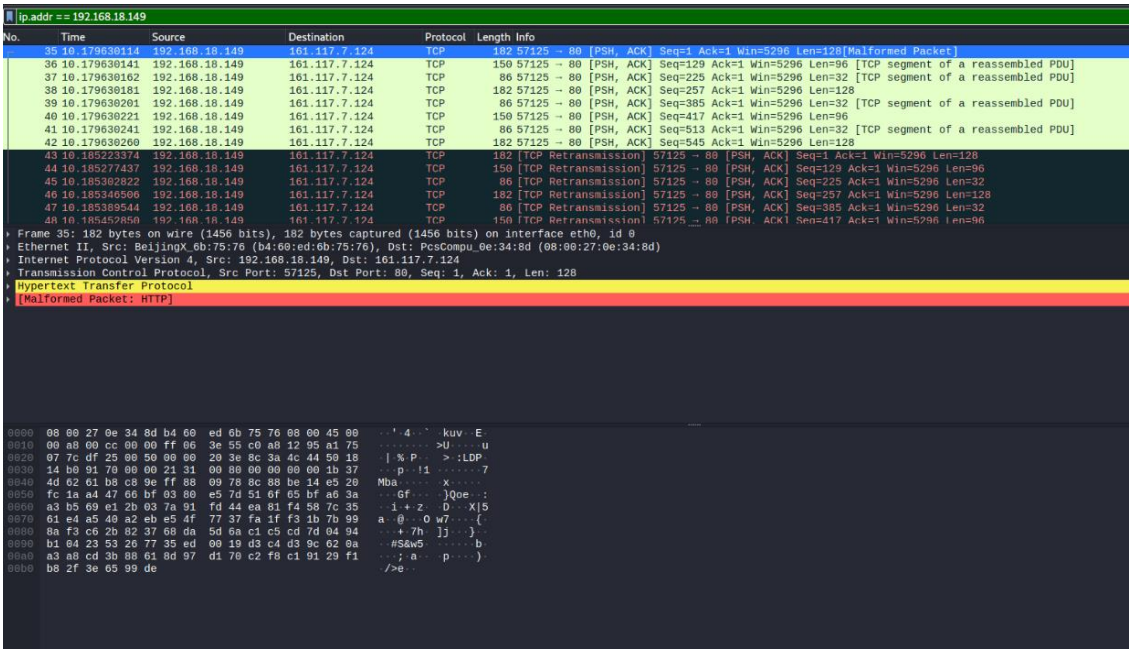

Figure 4-7 Communication between router and smart bulb

4.2.2 IP Smart Camera

4.2.2.1 ARP Poisoning

We start of by starting up the Ettercap tool in Kali Linux which we will use to perform man-in-the-middle attack on the Smart Camera.

Figure 4-8 Ettercap Interface

Connect to the network that the smart camera is on and click on ‘scan for hosts’ from the drop-down menu. A search will pop up and automatically search for all available hosts on the connected network.

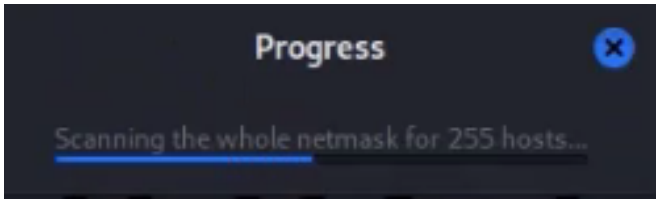

Figure 4-9 Scan for Hosts

All the scanned hosts can be viewed by clicking on ‘show hosts’ from the drop-down menu. All hosts will be displayed with their IP addresses and MAC addresses.

Figure 4-10 List of Hosts on network

- Add the smart camera as target 1 by manually searching for its IP address from the list.

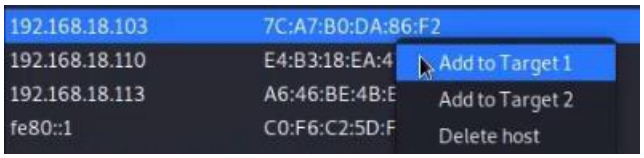

Figure 4-11 Adding Camera as target 1

- Add the router as target 2 by manually searching for the gateway IP from the list.

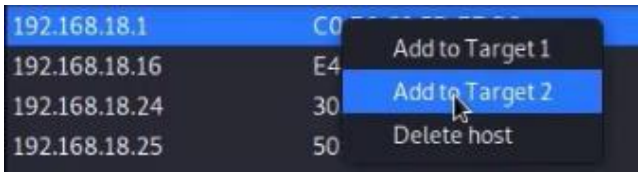

Figure 4-12 Adding Router as target 2

Begin ARP poisoning by selecting it from the drop-down menu. ARP poisoning is successful, and your device will be the man-in-the-middle between the smart camera and the router.

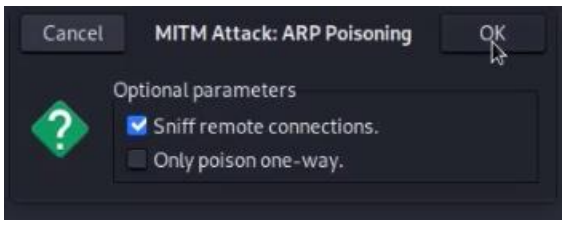

Figure 4-13 ARP poisoning

4.2.2.2 Traffic Analysis

Startup Wireshark tool in Kali Linux and select the option which has an active internet connection.

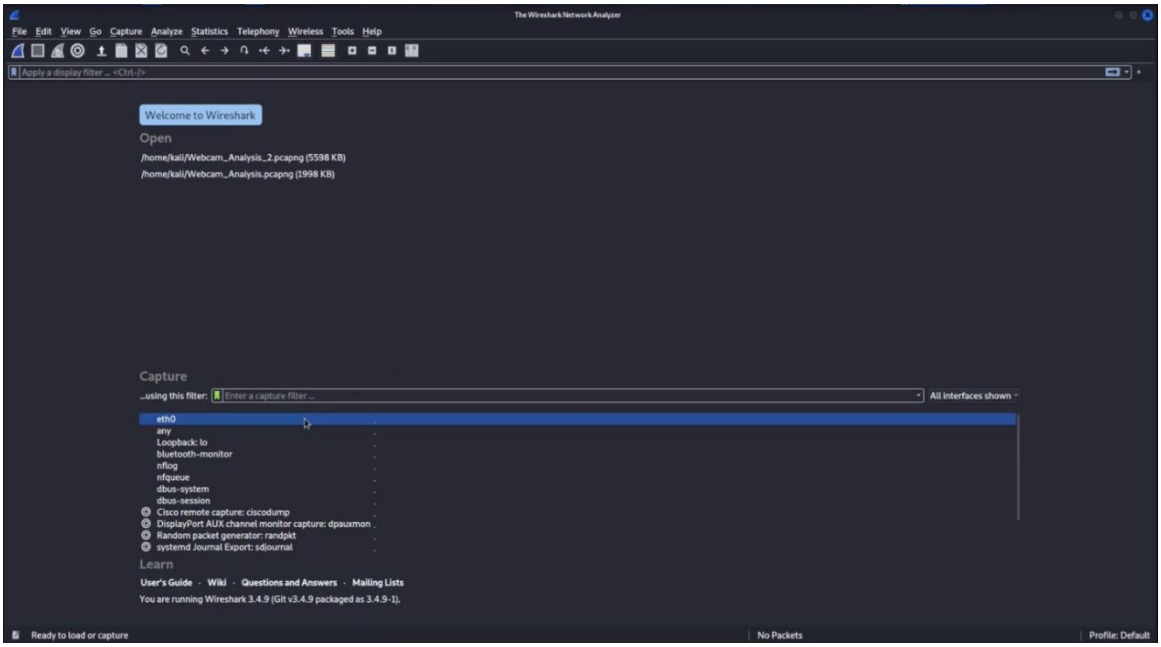

Figure 4-14 Wireshark interface

Now all the communication between the smart camera and the router will pass through your device. Enter the IP address of the smart camera in the filter available above so only the relevant communication is displayed and is visible for analysis.

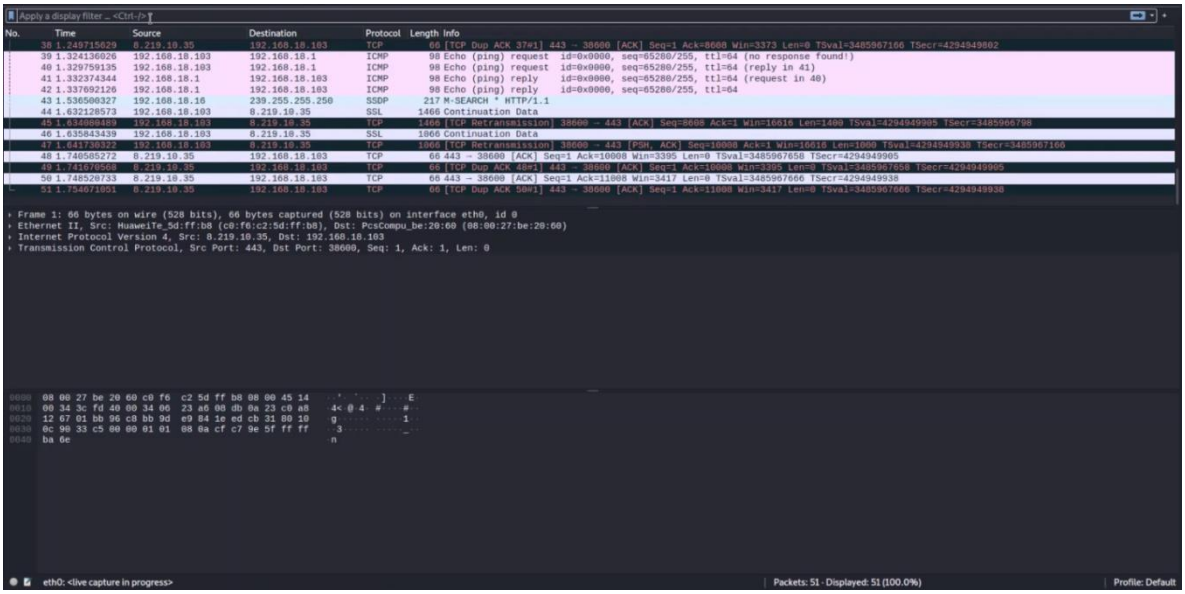

Figure 4-15 Communication between Camera and Router

4.2.2.3 Password Extraction

For password extraction enter the custom filter “udp.dstport == 7050 “ in the filter and wait for the user to login to the smart camera from his app. The packet carrying the username and password will be captured by Wireshark

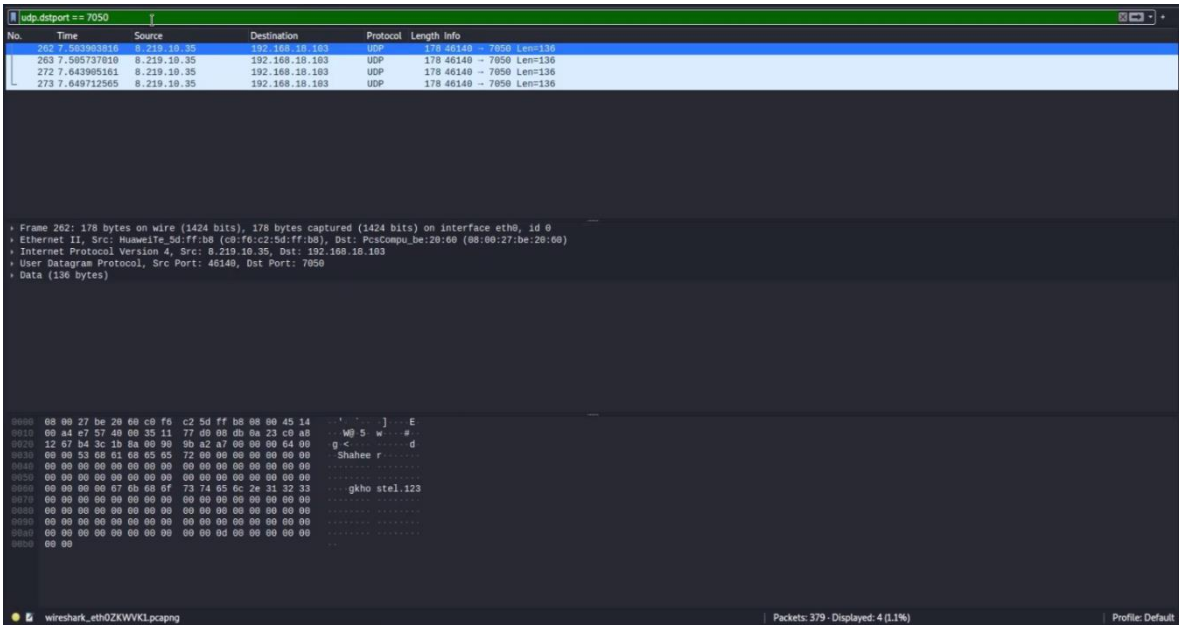

Figure 4-16 Password Extraction via filter

The username and password of the user that accessed the camera will be available in the packet description.

Figure 4-17 Password in packet description

4.2.2.4 Remote Access

The username and the password obtained in password extraction will be essential for remote access. We will use the following python script:

```
# import the opencv library

import cv2

# define a video capture object

vid = cv2.VideoCapture("rtsp://admin:Admin123@l92.168.18.19:554/11")

while:

        # Capture the video frame

# by frame
```

```
        ret, frame = vid.read()
        print(ret)
        # Display the resulting frame
        cv2.imshow('frame', frame)
        # the 'q' button is set as the
        # quitting button you may use any
        # desired button of your choice
        if cv2.waitKey(1) & OxFF == ord('q'):
            break
# After the loop release the cap object
vid.release()
# Destroy all the windows
cv2.destroyAllWindows()
```

After launching the script, a video link will be established, and you will see what the user sees

Figure 4-18(a) Output of python script

Figure 4-18(b) Remote Access of camera on laptop

4.2.2.5 Denial of Service

Denial of service is an interruption in an authorized user's access to a computer..network, typically caused by malicious intent. A DoS attack is possible using Xerxes, a tool in Kali Linux. The hacker The Jester (th3j35t3r) created Xerxes, an incredibly effective DoS tool for automating DoS attacks. It allows you to launch several separate attacks against multiple target sites without the need for a botnet. Startup multiple windows on Kali Linux with the command ./xerxes #targer IP [space] port no; where the target IP will be the camera with the port number being 554, which is permanently open.

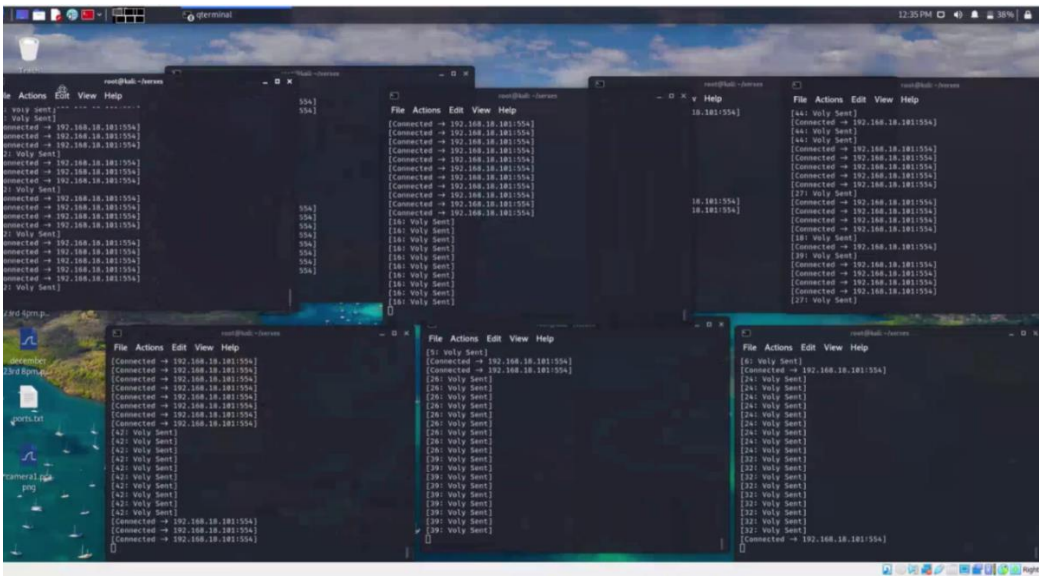

Figure 4-19 Multiple Xerxes Windows in Operation

After a while, the app connected to the smart camera will start lagging and will subsequently stop responding

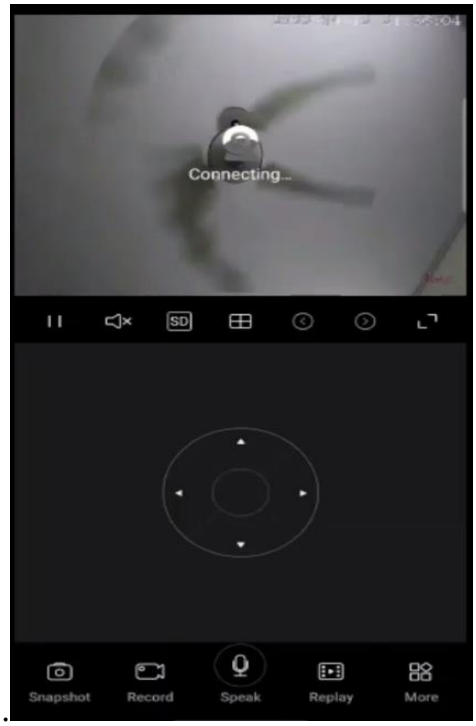

Figure 4-20(a) Response of app

Quitting and restarting the app will not help and it will continue to be non-responsive as long as the DoS is active using XerXes on Kali Linux.

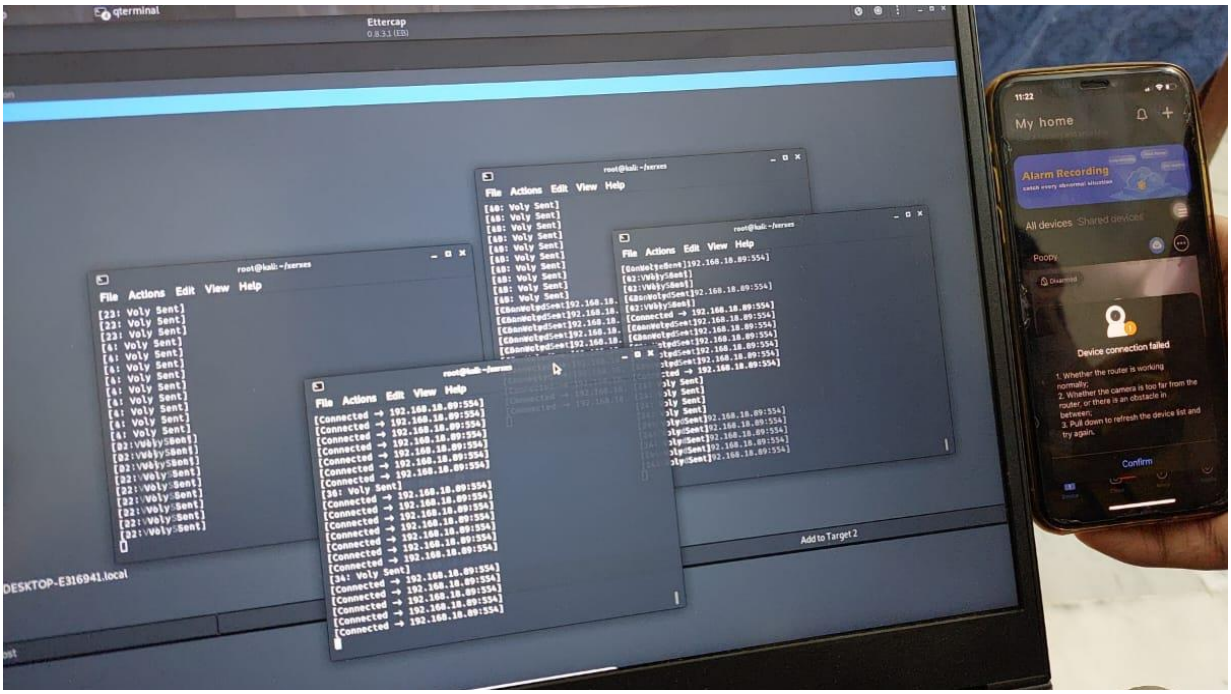

Figure 4-20(b) App unresponsive while Xerxes active

4.3. Chapter Summary

We have successfully launched a variety of attacks such as DoS and ARP spoofing on our procured devices. The chapter gave detailed step by step of how we did it.

CHAPTER 5: REMEDIAL MEASURES

CHAPTER 05

REMEDIAL MEASURES

5.1. Chapter Overview

This chapter focuses on stage 3 of our project, in which we have to secure the procured devices. The details will be discussed on how to secure our smart devices from intruder.

5.2. Stage 3: Remedial Measure after Analysis of attack

The main aspect of safeguarding devices is the raspberry pi. The Raspberry Pi Foundation, in collaboration with Broadcom, developed a series of miniature single-board computers in the United Kingdom. The Raspberry Pi project was created with the goal of encouraging the teaching of basic computer science in schools and disadvantaged countries. What we will need to bring this into actuation is:

- Raspberry Pi
- Ethernet cable
- SD Card (4GB or greater)
- Micro-SD card reader
- Power supply for your Pi & a Micro USB cable USB
- Case for your Pi (optional)

5.2.1. Setting up Raspberry Pi

To get Raspberry Pi OS to work on our Raspberry Pi Compute Module 4, we'll need to flash it first. First, use a micro-SD card reader to connect a micro-SD card to your computer, then download the Raspberry Pi Imager for your operating system. Open the Raspberry Pi Imager programme and select the newest version of the Raspberry Pi OS under CHOOSE OS.

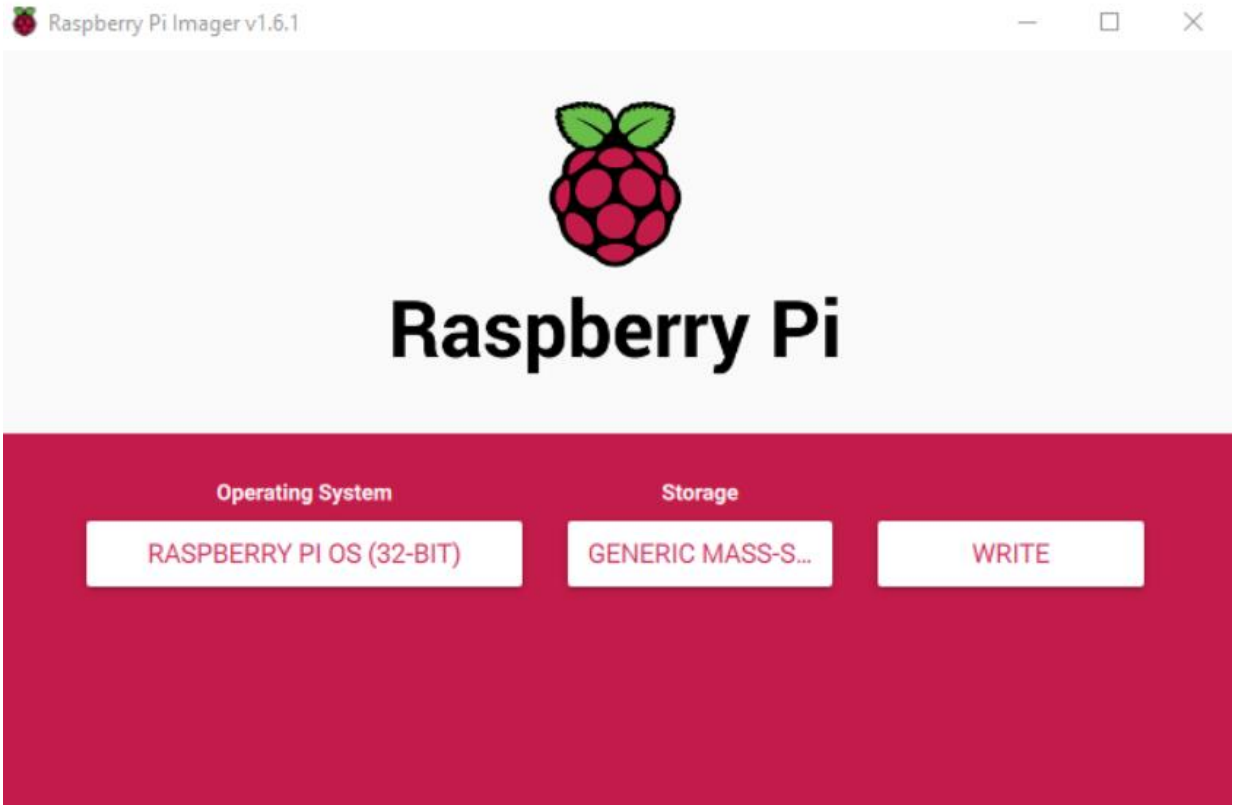

Figure 5-1 Raspberry Installation

Click CHOOSE STORAGE and select the connected micro-SD card and finally, click WRITE. The flashing should continue in a few minutes and writing will be complete.

5.2.2. Securing Raspberry Pi

After all the necessary set-up is done and the raspberry pi is up and running (fig 2).

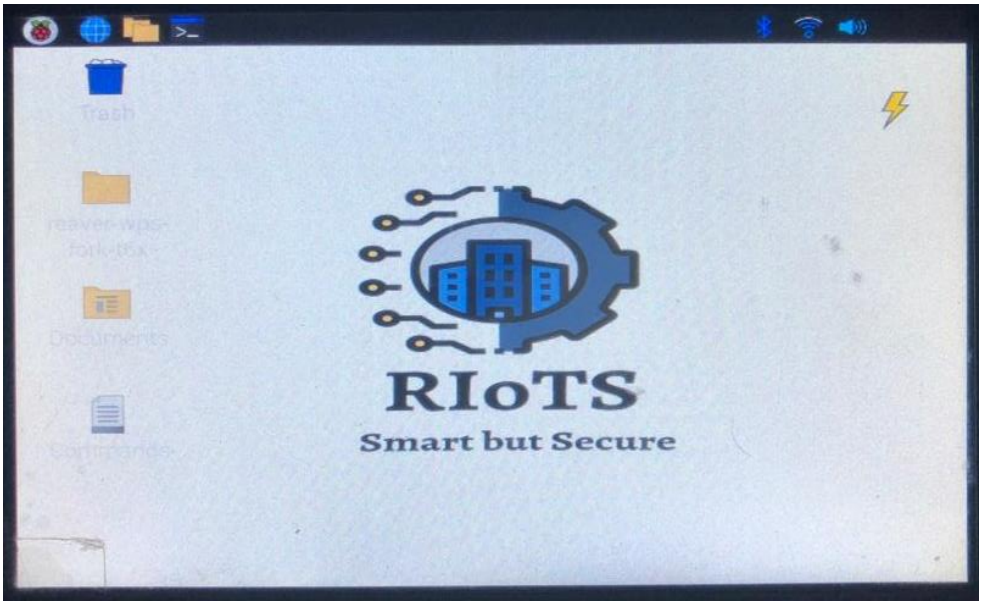

Figure 5-2 Raspberry Installation

Next comes to secure the raspberry pi from a network standing point. For this we close all the open ports including SSH access and RDP access. This can be done by in the following way:

1. List open ports:

   netstat -lnt

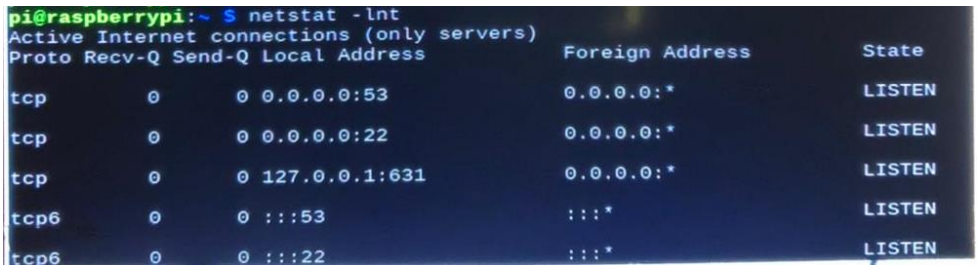

Figure 5-3 Open Ports

Filtered:

For tcp: netstat -lnt | grep LISTEN | awk '{ print ($4) }' | awk 'BEGIN{FS=":"} { print $(NF) }' | sort -n | uniq

For udp: netstat -lnt | grep udp | awk '{ print ($4) }' | awk 'BEGIN{FS=":"} { print $(NF) }' | sort -n | uniq

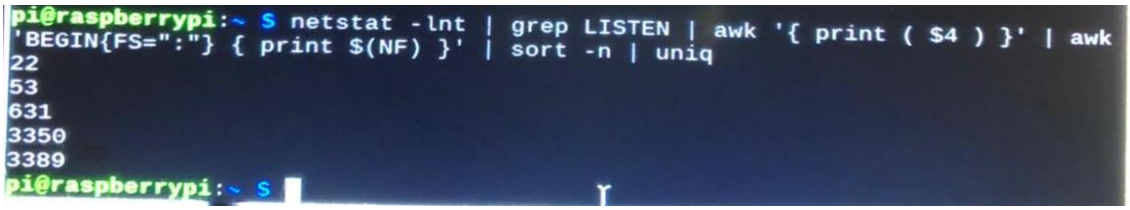

Figure 5-4 Script

2. Close all the unnecessary ports or in technical terms to “kill” the open ports using the following commands:

   kill port already in use: kill -9 $(lsof -i tcp:3000 -t)

   kill a port: kill $(lsof -ti:3000)

3. Change SSH default port and use SSH keys instead of passwords. SSH default port is 22. Edit the SSH server configuration file:

   sudo nano /etc/ssh/sshd_config

   Find this line:

   #Port 22

   Replace the port with the one you want to use, and make sure to uncomment the line:

   Port 1111

   Save and exit (CTRL+O, CTRL+X)

Restart you Server:

sudo service ssh restart

Then we generate a key on the computer, and then add it to the Raspberry Pi to allow a connection from the computer.

5.2.3. Connecting Raspberry and Camera

Now, after securing the raspberry pi, the aim will be to cause the packets of the IP camera pass through the raspberry which will in its place interact with the internet. It will look something like this.

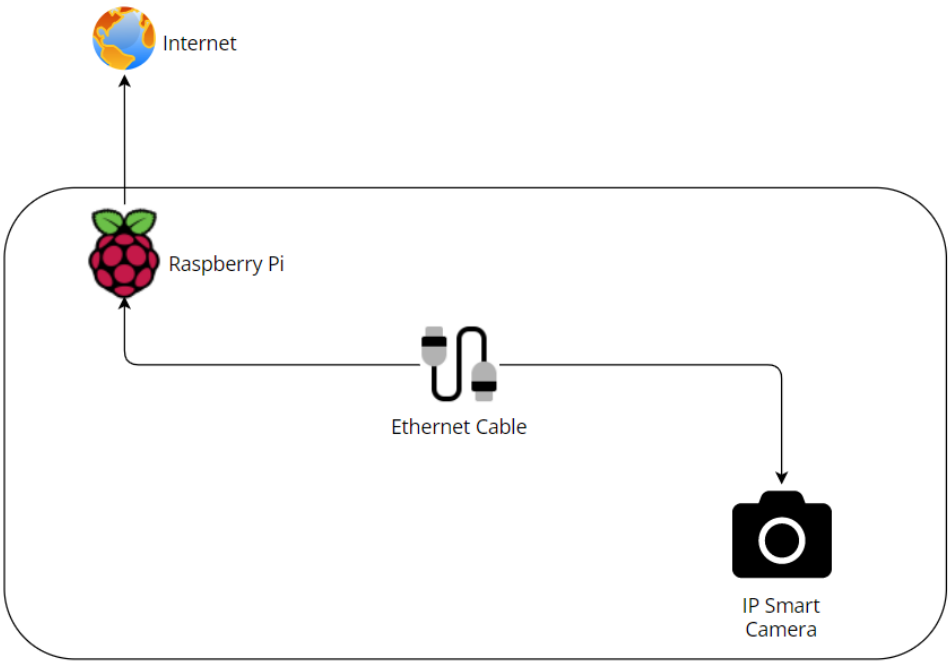

Figure 5-5 Connection of Raspberry with IP Camera

For this we will require an ethernet cable and connect it to the IP smart camera and he raspberry pi. However, this will not be enough to provide the IP camera with Internet. We will run the following script and that will allow us to provide internet access to the IP smart camera

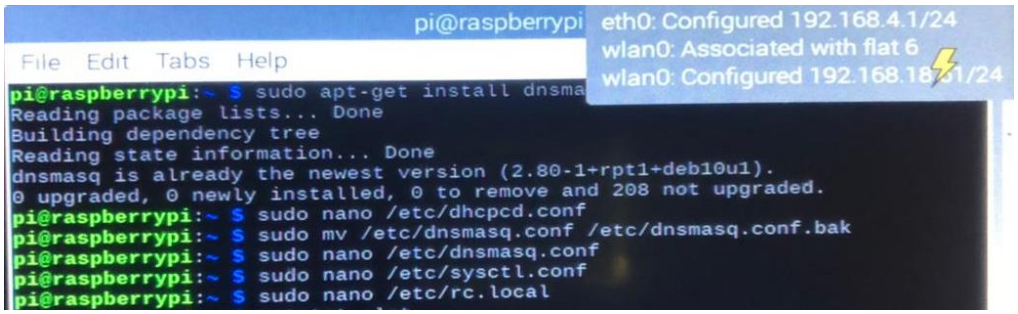

Figure 5-6 Script file to provide access to camera

With this done, the IP smart camera will connect to the server and start responding on the app

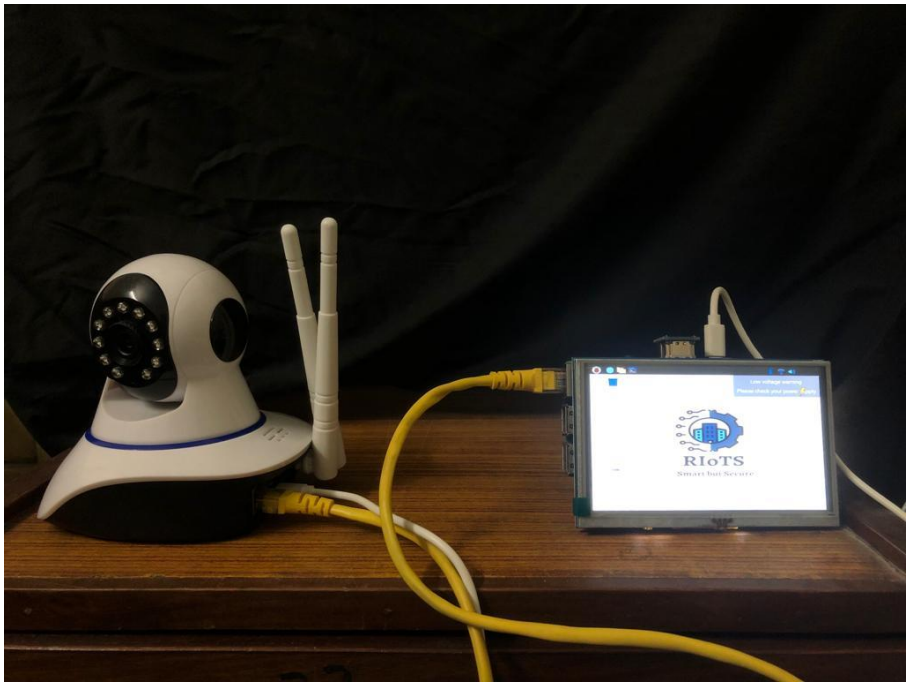

Figure 5-2 IP Camera and Raspberry connected via Ethernet

5.3. Chapter Summary

We secure the IP camera by using raspberry pi. In doing this, the raspberry pi is effectively acting as the stand in for the IP camera in the network and as a result keeping it safe from hackers. Scanning the network in any way does not show the IP smart camera as a host and hence keeping it safeguarded.

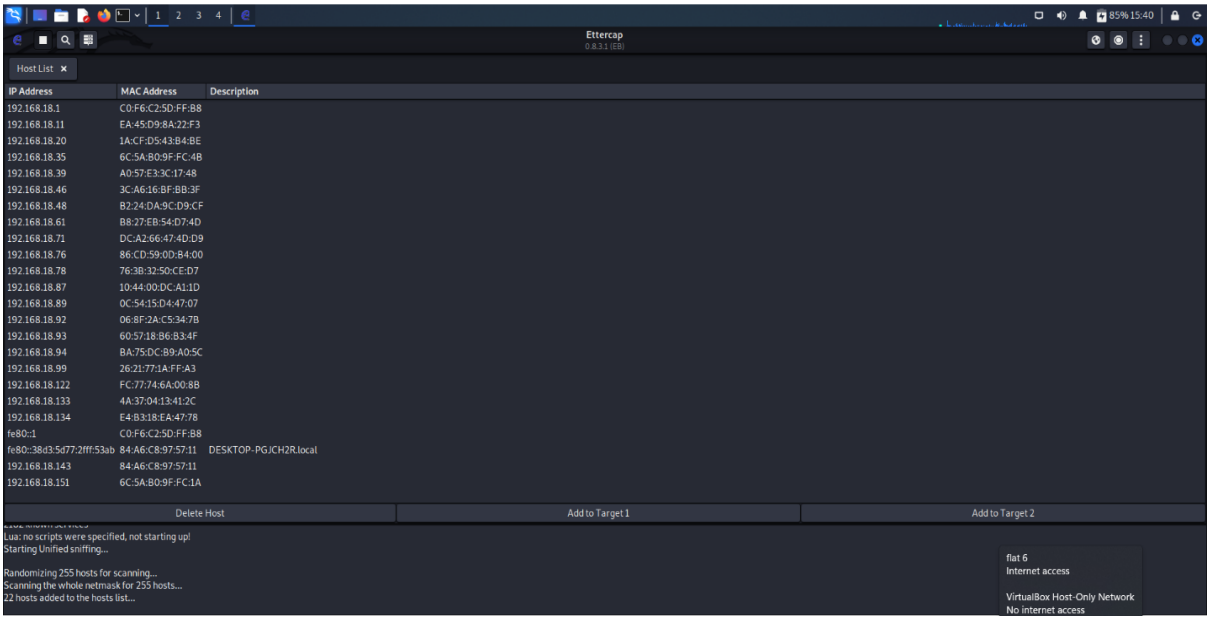

Figure 5-3 Network Scan

As it can be seen the MAC address of the IP camera (7C:A7:B0:DA:86:F2) is not displaying upon scanning even though we are on the same network as the IP smart camera.

CHAPTER 6: CONCLUSION AND ENHANCMENETS

CHAPTER 06

CONCLUSION AND ENHANCEMENTS

6.1. Chapter Overview

The following chapter elucidates the enhancements and future work to be performed in order to render RIoTS more secure and advanced. It also concludes the whole document consists of RIoTS complete information.

6.2. Conclusion

According to the recently survey conducted in which about 21 organizations that consisted of jazz, Ufone MIS cell etc. We asked them have your organizational equipment involve IoT are secure or have you aware of any service that providing security to your organizational data. On which 92% answered No. Now this whole is a lot to accomplish ,so we in our limited scope, could get a hold of relatively limited and inexpensive IoT devices which actually act as a building block of smart cities.

Features	RIoTS
Real time information	✓
Data privacy	✓
IoT Device security	✓
secrecy	✓

When we talk about sustainable smart cities then encompass smart transportation, smart agriculture, smart homes. Now this whole is a lot to accomplish, so we in our limited scope, could get a hold of relatively limited and inexpensive IoT devices which actually act as a building block of these smart cities.

For instance, in the smart cities of Gwadar, Karachi and swat there are definitely cameras and lightening systems and in smart homes people have air conditioners, simply people wanting to smooth to better their lives. In a general environment these IoT devices communicate with their routers gateway towards the internet. Now they are communicating a lot valuable & critical user data without check, so our solution works in a way that it ensures real-time IoT security, the solution sits behind these devices and the network gateway in order to analyze what information goes out of the network, and how it works basically is that captures the traffic and analysis that, sees if there are weak passwords that can be compromised, it checks whether devices are vulnerable to DoS attacks, whether remote code can be executed over them, whether the communication their using with the rest of the internet is unencrypted or not, if information is being leaked and whether there are configuration issues that the attacker can exploit because even one of these internal IoT device is compromised then it will act as a pivot point to launch wider range of attacks on rest of the IoT network. Now this is the overall technical working of the device, and besides this RIoTS can work in a different fashion as well by just checking the security configurations, the passwords and encryption and all that stuff of the in its individuality without being applied to the network.

6.3. Enhancements and Future Work

- RIoTS meaning it can be applied on a whole network and also a device can be tested under the umbrella of RIoTS to reveal its weaknesses, it can analyze network traffic in real time, it covers wide range of attacks.
- This product requires basic technical knowledge with no extensive training required that the on-hand network administrator can handle it.
- RIoTS can work in a different fashion as well by just checking the security configurations, the passwords and encryption and all that stuff of the in its individuality without being applied to the network

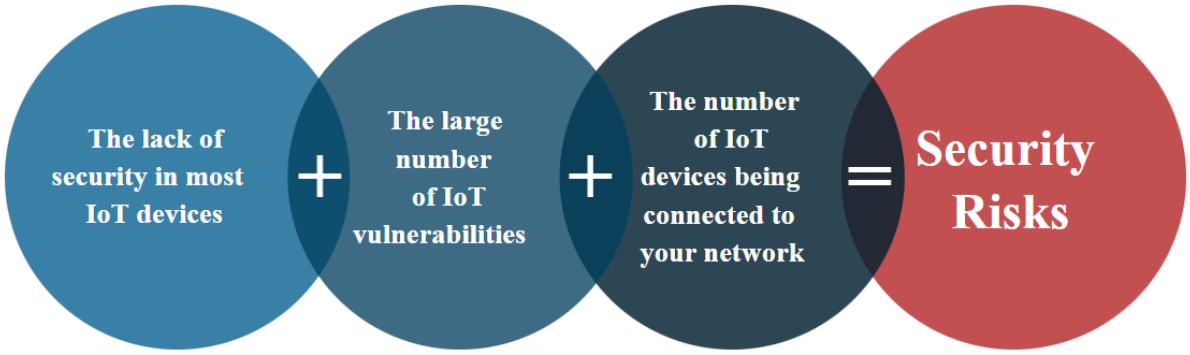

Figure 6-1 Security Risks

6.4. Chapter Summary

The current section concludes the thesis by implying the future work to be done in order to enhance the scope of our project and summarizes the entire documentary by shedding light on the core and important characteristics of the conversed project, RIoTS.

REFERENCES:

[1] ieeexplore.ieee.org/abstract/document/8697723

[2] ijariie.com/AdminUploadPdf/SMART_BULB_USING_IOT_ijariie9666.pdf

[3] ieeexplore.ieee.org/abstract/document/7804660

[4] Khalid Shahbar A. Nur Zincir-Heywood, "Benchmarking Two Techniques for IoT Classification, Flow Level and Circuit Level attacks ", from Faculty of Computer Science, Dalhousie University, Halifax, Canada

[5] Jia Lingyu, Liu Yang, Wang Bailing, Liu Hongri, Xin Guodong, "A Hierarchical Classification Approach for Tor Anonymous Traffic analysis", in Proceedings of the 2017 9th IEEE International Conference on Software and Network security.

[6] Priya Mayank, A. K. Singh, "IoT devices Traffic Identification", in Proceedings of the 2017 7th International Conference on Communication Systems and Network Technologies.

[7] Khalid Shahbar, A.Nur Zincir Heywood, "Traffic Flow Analysis of IP camera".

[8] https://www.techrepublic.com/article/report-smart-bulbs-have-a-major-security-problem/

[9] https://www.techrepublic.com/topic/security/

[10] https://www.techrepublic.com/topic/tech-and-work/

[11] https://www.researchgate.net/publication/344490696_Smart_Lamp_or_Security_Camera_Automatic_Identification_of_IoT_Devices

[12] Ibrahim Ghafir *, Jakub Svoboda † and Vaclav Prenosil, "IOT-BASED MALWARE", * Faculty of Informatics, Masaryk University† Institute of Computer Science, Masaryk University Brno, Czech Republic.

[13] https://opensource.com/resources/linux

[14] https://www.quora.com/What-is-socket-programming-a-socket-server-and-a-socket-client

[15] https://en.wikipedia.org/wiki/Windows_10

[16] https://www.plesk.com/blog/various/what-is-linux/

[17] Khalid Shahbar, A.Nur Zincir Heywood, "Traffic Flow Analysis of TOR Pluggable Transports".

Riots Final

ORIGINALITY REPORT

13%	11%	7%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.riverpublishers.com Internet Source	2%
2	www.scribd.com Internet Source	1%
3	digital.library.ucf.edu Internet Source	1%
4	Yogeesh Seralathan, Tae Tom Oh, Suyash Jadhav, Jonathan Myers, Jaehoon Paul Jeong, Young Ho Kim, Jeong Neyo Kim. "IoT security vulnerability: A case study of a Web camera", 2018 20th International Conference on Advanced Communication Technology (ICACT), 2018 Publication	1%
5	origin.geeksforgeeks.org Internet Source	1%
6	www.coursehero.com Internet Source	1%
7	raspberrytips.com Internet Source	1%

8	Submitted to Higher Education Commission Pakistan Student Paper	<1 %
9	www.honorbuy.com Internet Source	<1 %
10	iarjset.com Internet Source	<1 %
11	Jeff Cicolani. "Beginning Robotics with Raspberry Pi and Arduino", Springer Science and Business Media LLC, 2021 Publication	<1 %
12	dir.indiamart.com Internet Source	<1 %
13	spectrum.library.concordia.ca Internet Source	<1 %
14	industrialinternetofthings.home.blog Internet Source	<1 %
15	dx.doi.org Internet Source	<1 %
16	ijisrt.com Internet Source	<1 %
17	onlinelibrary.wiley.com Internet Source	<1 %
18	open.library.ubc.ca Internet Source	<1 %

19	scholar.ppu.edu Internet Source	<1 %
20	samenacouncil.org Internet Source	<1 %
21	udemycoupon.learnviral.com Internet Source	<1 %
22	Mohamed Abomhara, Geir M. Koien. "Security and privacy in the Internet of Things: Current status and open issues", 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), 2014 Publication	<1 %
23	www.r4igold.co.za Internet Source	<1 %
24	hdl.handle.net Internet Source	<1 %
25	mafiadoc.com Internet Source	<1 %
26	repository.wit.ie Internet Source	<1 %
27	repository.nwu.ac.za Internet Source	<1 %
28	Mohamed Abomhara, Geir M. K[illegible]ien. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and	<1 %

Attacks", Journal of Cyber Security and Mobility, 2015
Publication

29	"Smart Sensors at the IoT Frontier", Springer Science and Business Media LLC, 2017 Publication	<1%
30	Orlando Arias, Jacob Wurm, Khoa Hoang, Yier Jin. "Privacy and Security in Internet of Things and Wearable Devices", IEEE Transactions on Multi-Scale Computing Systems, 2015 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		