

SENIOR YEAR PROJECT REPORT

BY: TH33GROOT

IoT
PROJECT

2017

PORTABLE
SURVEILLANCE AND
NETWORK
MONITORING
SYSTEM



DECLARATION OF ORIGINAL WORK

“I certify that the material contained in this proposal is my own work and does not contain unreferenced or unacknowledged material. I also warrant that the above statement applies to the implementation of the project and all associated documentation. Regarding the electronically submitted version of this submitted work, I consent to this being stored electronically and copied for assessment purposes, including the Department’s use of plagiarism detection systems in order to check the integrity of assessed work. I agree to my dissertation being placed in the public domain, with my name explicitly included as the author of the work.”

Date: 8th December 2017

kamandepeternumi

DEDICATION

I dedicate this research paper to Raphael Clementina Muendi for always being there for me, believing in me and assisting me.

ACKNOWLEDGMENTS

I would like to take this opportunity to express my gratitude to my supervisor Dr. Paul Okanda, for his continuous support and guidance.

I would also like to thank my family; Mr. James Kimani Numi and Mrs. Mary Wangare Numi for the continuous support, My friend and Brother Raphael Charles Ndolo for assisting me in the programming of the user interface of the system and suggestions on how to make the system more better and user friendly.

ABSTRACT

The main aim for this project is to provide an economical, user friendly and easy to set up surveillance and WiFi network monitoring system for home users with internet connection, to help and allow the users to monitor both activities happening on their homestead or surrounding and what is going through their network. In today's society with the growth of technology and inter-connectivity, many home users have found the need for having internet in their homes for either using it to do their work assignments from home, school assignments, and research studies or even for leisure use. With this internet connection do the users know what is going through their network or are they even aware if they are already compromised or not.

This system will allow the user to monitor his home surrounding and if any motion is detected when he/her is not around the area it will notify the user where he will also be able to monitor what is going through his network.

Table of Contents

CHAPTER 1: INTRODUCTION.....	9
CHAPTER 2: BACKGROUND.....	10
2.1 History of Surveillance Monitoring systems.....	10
2.2 History of Network Monitoring systems.....	10
2.3 Existing Systems.....	11
2.3.1 ANALOG CAMERA SURVEILLANCE.....	11
2.3.2 HONEY HOUSE PROJECT.....	12
2.3.3 WIRE SHARK SOFTWARE PROGRAM.....	13
2.3.3.4 PROBLEM STATEMENT FROM THE EXISTING SYSTEMS.....	14
2.3.3.4.1 EXISTING SYSTEM COMPARISON TABLE.....	14
CHAPTER 3: AIMS AND OBJECTIVES.....	15
CHAPTER 4: PROPOSED PROJECT.....	15
CHAPTER 5: METHODOLOGY.....	15
Phase One.....	15
Suggest project idea -.....	15
Proposal writing -.....	15
.....	15
Phase Two.....	16
Requirements Gathering -.....	16
System Testing -.....	16

Phase Three.....	16
First project presentation -.....	16
Website system design -.....	16
Website system testing -.....	16
Phase Four.....	17
Full system implementation -.....	17
Phase Five.....	17
Project write up -.....	17
Final project presentation –.....	17
PROJECT MANAGEMENT NETWORK DIAGRAM.....	17
CHAPTER 6: DESIGN.....	20
6.1 USE-CASE DIAGRAM.....	20
6.2 ENTITY RELATIONSHIP DIAGRAM.....	21
6.3 DATA FLOW DIAGRAM.....	22
6.3.1 USER:.....	22
6.3.2 ADMIN:.....	23
6.4 FLOW CHART.....	24
6.4.1 USER:.....	24
CHAPTER 7: IMPLEMENTATION.....	26
7.1 THE SURVEILLANCE MONITORING SYSTEM.....	26
7.2 THE NETWORK MONITORING SYSTEM.....	28

7.3 WEB INTERFACE.....	30
7.3.1 USER WEB INTERFACE.....	31
7.3.2 ADMIN WEB INTERFACE.....	35
7.4 INTERNET CONNECTION.....	39
CHAPTER 8: CHALLENGES.....	41
8.1 LOW END DEVICES.....	41
8.2 COST.....	41
8.3 HONEYPOT DEPLOYMENT.....	41
CHAPTER 9: EVALUATION.....	42
9.1 TEST: SURVEILLANCE AND NETWORK MONITORING SYSTEM COMPONENTS TEST.....	42
9.1.2 WEBCAM TEST: Turn on webcam indicator.....	42
9.1.3 WiFi ADAPTERS TEST: Turn on webcam indicator.....	43
CHAPTER 10: CONCLUSION.....	45
10.1 FUTURE WORK.....	45
REFERENCES.....	46
GLOSSARY.....	47
APPENDIX 1: SIGNED LOG BOOK.....	48
APPENDIX 2: CONFIG FILES.....	56

CHAPTER 1: INTRODUCTION.

What is monitoring? In general this is the action of observing and checking the progress or quality of (something) over a period of time. Narrowing down to monitoring definitions in accordance to the context of the topic surveillance monitoring is the monitoring of behavior, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people (Lyon, 2007), this can include observation from a distance by means of electronic equipment (such as closed-circuit television (CCTV) cameras) (Kille & Maximino, 11 February 2014) while network surveillance is the is the monitoring of computer activity and data stored on a hard drive, or data being transferred over computer networks such as the Internet. The monitoring is often carried out covertly and may be completed by governments, corporations, criminal organizations, or individuals (Wikipedia, 2017).

The evolution of technology and inter-connectivity which has adapted as the needs of its community have changed has grown and most users in the community have seen the need of internet access from their homes. The main question comes to this, do all internet users know what is happening within their network? Few of them with the computer and networking skills will know, but the rest of them who do not have the skills will not have any idea around this.

Internet connection has allowed new type of malicious activity that has lead to destroying organizations, people's lives and even a nation itself. All this occur because the users are the representatives of these places, and yet we are the weakness of all this systems and places. When a user has been hacked¹ it occurred either when he/she was in the internet either at home, work or public environment. The attacker the person also known as the hacker² is able to steal data or manipulate the user's devices through the internet from a different location by a click of a button.

Stuxnet worm entered Iran's nuclear facilities through hacked suppliers



Jon Fingas, @jonfingas
11.13.14

6
Comments

84
Shares



Fig1. An article on the worm that is now known as a cyber weapon, the worm infected the most secure infrastructure through hacked suppliers and was discovered after a couple of years of it being in the system, destroying its target and spreading beyond it intended target after destroying its target (Fingas, 2014).

This is the main reason why an internet user have to get to know what is going through or in their home network and with this system, it will allow a user to know if his network faced any cyber-attacks, and notify him/her if there is unauthorized access in the location or place he wants to monitor and most of all it will be user friendly.

1 Hacked; verb: hack is to circumvent security and break into (a network, computer, file, etc.), usually with malicious intent.

2 Hacker: Originally in computing it meant a skilled computer expert that uses his or her computing technical knowledge to solve a problem, but nowadays it is skilled computer expert that uses his or her computing technical knowledge to gain unauthorized access to data or a system.

CHAPTER 2: BACKGROUND.

2.1 History of Surveillance Monitoring systems.

Although current modes and technologies of surveillance seem to suggest that surveillance is a product of the 21st century, there are countless examples of surveillance activities occurring throughout history (wikipedia, 2016).

Keith Laidler proposes in his book Surveillance Unlimited: How We've Become the Most Watched People on Earth, "spying and surveillance are at least as old as civilization itself (wikipedia, 2016).

In history, surveillance is often referred to as spying or espionage. Most often, surveillance historically occurred as a means to gather and collect information, supervise the actions of other people (usually enemies), and to use this information to increase one's understanding of the party being spied on. Sometimes, surveillance occurred most often through the use of an individual spy, or a small group of spies. As technology such as spyglasses, telescopes and radios developed, surveillance technologies continually affected the way in which surveillance occurred. Modern surveillance technologies such as CCTV, RFID and GPS help to highlight the extent to which surveillance practices have evolved throughout history (wikipedia, 2016).

2.2 History of Network Monitoring systems.

Network monitoring is a difficult and demanding task that is a vital part of a Network Administrator's job. Network Administrators are constantly striving to maintain smooth operation of their networks. If a network were to be down even for a small period of time productivity within a company would decline, and in the case of public service departments the ability to provide essential services would be compromised. In order to be proactive rather than reactive, administrators need to monitor traffic movement and performance throughout the network and verify that security breaches do not occur within the network (Cecil, 2006).

Network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network." -Orebaugh, Angela. Two Monitoring Techniques are discussed in the following sections: Router Based and Non-Router Based. Monitoring functionalities that are built-into the routers themselves and do not require additional installation of hardware or software are referred to as Router Based techniques. Non-Router based techniques require additional hardware and software to be installed and provide greater flexibility (Cecil, 2006).

2.3 Existing Systems.

During research I found some existing systems similar to my systems objective and aims, but I will state their pros and cons.

2.3.1 ANALOG CAMERA SURVEILLANCE



Fig 2. Third party company installing an analog camera (Camera, 2015).

This is a normal third party analog camera installation, It is a system that uses cable to transmit the feed and a DVR's to record the feed as it is being transmitted.

The value for all the accessories and installation will range at different price range due to either what type of accessories would you prefer either low end or high end, distance from focus area and the third party company installation prices.

The Pros are

- ✓ They are reliable
- ✓ Easy to installation
- ✓ Easy to operate
- ✓ Compatible with all standard power/ video BNC (round) connectors
- ✓ When combined with the digital video recorders you can easily watch your cameras remotely live and review past video on your pc, Cell phone or tablet.

The Cons are

- x They are stationary mounted at one point
- x They require some technical knowledge during installation
- x They are noticeable
- x Users being forced to have third party doing the system installation, the third party being greedy will tend to overprice hence scamming³ the user.

³ Scam: is a dishonest scheme.

2.3.2 HONEY HOUSE PROJECT

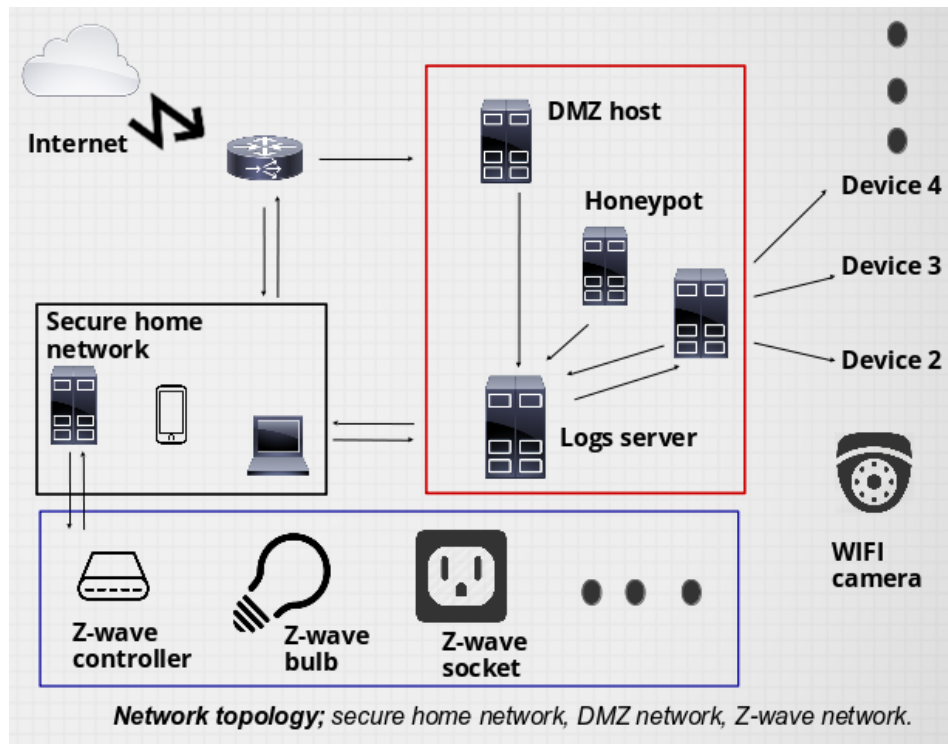


Fig 3. Honey House project setup (AfricaHackOn, 2017).

This was a system that had an intersection of three disciplines; home automation, honeypot concept and log analysis. Peter Ouma the project owner had this idea to setup a damn vulnerable home automation system, where he also created a mobile app for accessing the camera(for surveillance) and home automation system.

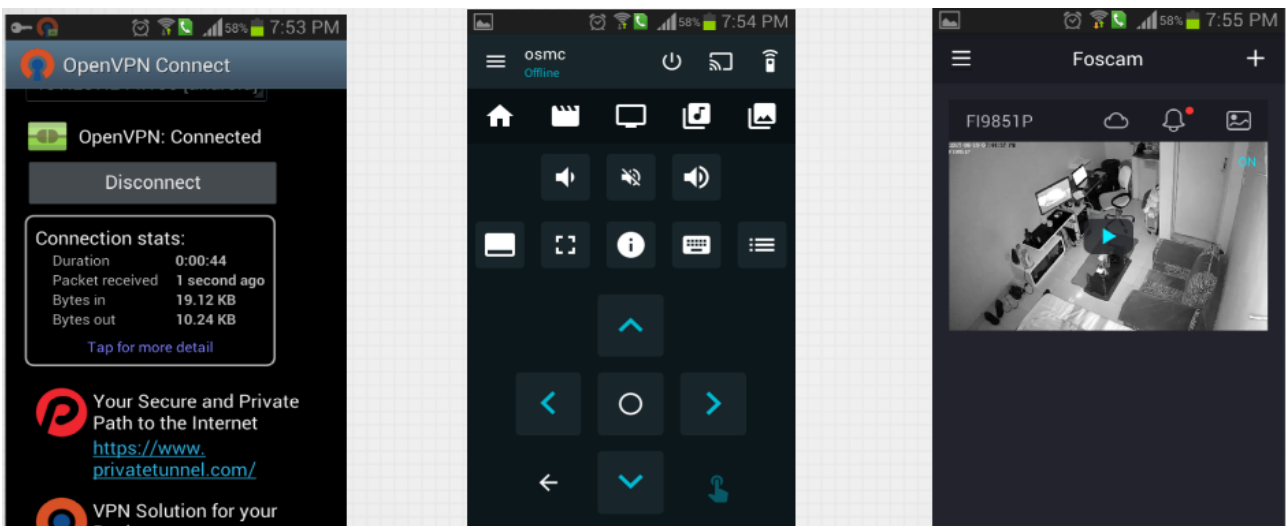


Fig 4. Honey House mobile app enabling access (AfricaHackOn, 2017).

The Pros are

- ✓ Connected to WiFi and the smart devices
- ✓ Easy to operate

The Cons are

- x The surveillance camera is stationary at one point
- x It requires technical knowledge and skills for installation
- x It is expensive (the SMART devices are costly)

2.3.3 WIRE SHARK SOFTWARE PROGRAM

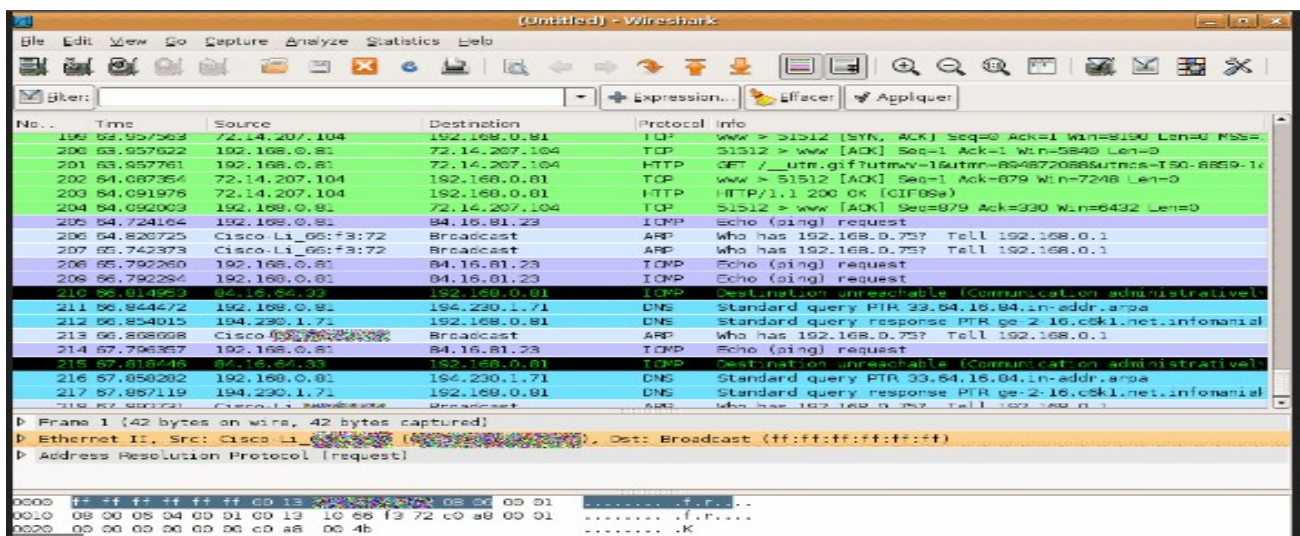


Fig 5. Wireshark Program that requires one to have computer skills and networking theory to use it (openmانيك, 2010).

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006.

The software basically sniffs packets actively when in transit and displays the time of transit wire, destination protocol and information carrying though a user requires networking skills and knowledge to use it.

The Pros are

- ✓ Easy installation process.
- ✓ Universal compatibility with all Operating Systems
- ✓ It is free

The Cons are

- x Requires networking skills and knowledge to operate

2.3.3.4 PROBLEM STATEMENT FROM THE EXISTING SYSTEMS

From the existing system we can see the main cons of these existing systems are:

- i. Cost
- ii. Ease of use
- iii. Portability
- iv. Compatibility of both surveillance and network monitoring systems into one.

2.3.3.4.1 EXISTING SYSTEM COMPARISON TABLE

	ANALOG CAMERA	HONEY HOUSE	WIRE SHARK SOFTWARE
Cost (relatively)	Expensive	Expensive	Cheap
Easy Installation	YES	NO	YES
Ease of use	YES	YES	NO
Portability	NO	NO	YES
Compatibility of both surveillance and network monitoring system in one	NO	YES	NO
Remote access	YES (when combined with a digital video recorders)	YES	NO
Continuous internet connection	YES	YES	YES

CHAPTER 3: AIMS AND OBJECTIVES.

The aims and objectives of the home surveillance and network monitoring system within the scope of the project to address the challenges of the existing system such as cost installation and setup of the system, ease of use with minimum knowledge and provide guides for usage and portability.

The objectives are as follows:

- I. To provide user friendly user interface for accessing the system functionalities.
- II. Combine both network monitoring and surveillance monitoring in one whole system.
- III. Implement a portable system.

CHAPTER 4: PROPOSED PROJECT.

The purpose of the project is to make a home surveillance and network monitoring system that will be cheaper than existing systems. This system will have a computer (Raspberry Pi) that is basically the host of the surveillance and network monitoring system. The computer will be used to host both systems and their programs where they will be started from the terminal or during the system startup.

CHAPTER 5: METHODOLOGY.

Phase One

Suggest project idea -

This was where the lecturer gets an idea of the project through word of mouth. I thought up the idea of doing a home surveillance and network monitoring system. I did all the required research on it and proposed it to my supervisor.

Proposal writing -

This is where the official proposal for the approved project is written. In this case it is the proposal for My Home Surveillance and Network Monitoring System which was handed in and reviewed by my supervisor and I.

Phase Two

Requirements Gathering -

This is where all the required hardware and software is gathered for the project to begin.

The said components are:

- Raspberry Pi 3 (preferably) \$ 50.00
- SD card storage 32GB \$ 10.00
- Raspberry Pi camera or USB Web Cam \$ 30.00
- External Power supply \$ 30.00
- HDMI to VGA converter \$ 4.00
- 2 USB cables @ \$ 1.00
- 2 WiFi Adapters @ \$ 30.00
- Router @ \$ 15.00

NB: One can use any raspberry pi model, Pi 3 is preferable due its processing capabilities is higher than the rest hence no lags, for the WiFi adapters one will be required to have two but one that can transmit in monitor mode.

Total cost range is approximately \$ 180.00 to \$ 201.00

System Design and Implementation -

This is where the RPi is coded with the camera to capture live feeds and snapshots of images and videos when motion is detected and host one of the other two tools for network monitoring.

System Testing -

This is where all the functions of the RPi working in conjunction with the camera and WiFi adapters are tested.

Phase Three

First project presentation -

This is where a presentation to show the progress of the project.

Website system design -

This is for the web user interface.

Website system testing -

This is where the functionality of the user interface is tested.

Phase Four

Full system implementation -

This is where the website and the RPi are linked and the testing of the whole system is done in preparation for the final presentation.

Phase Five

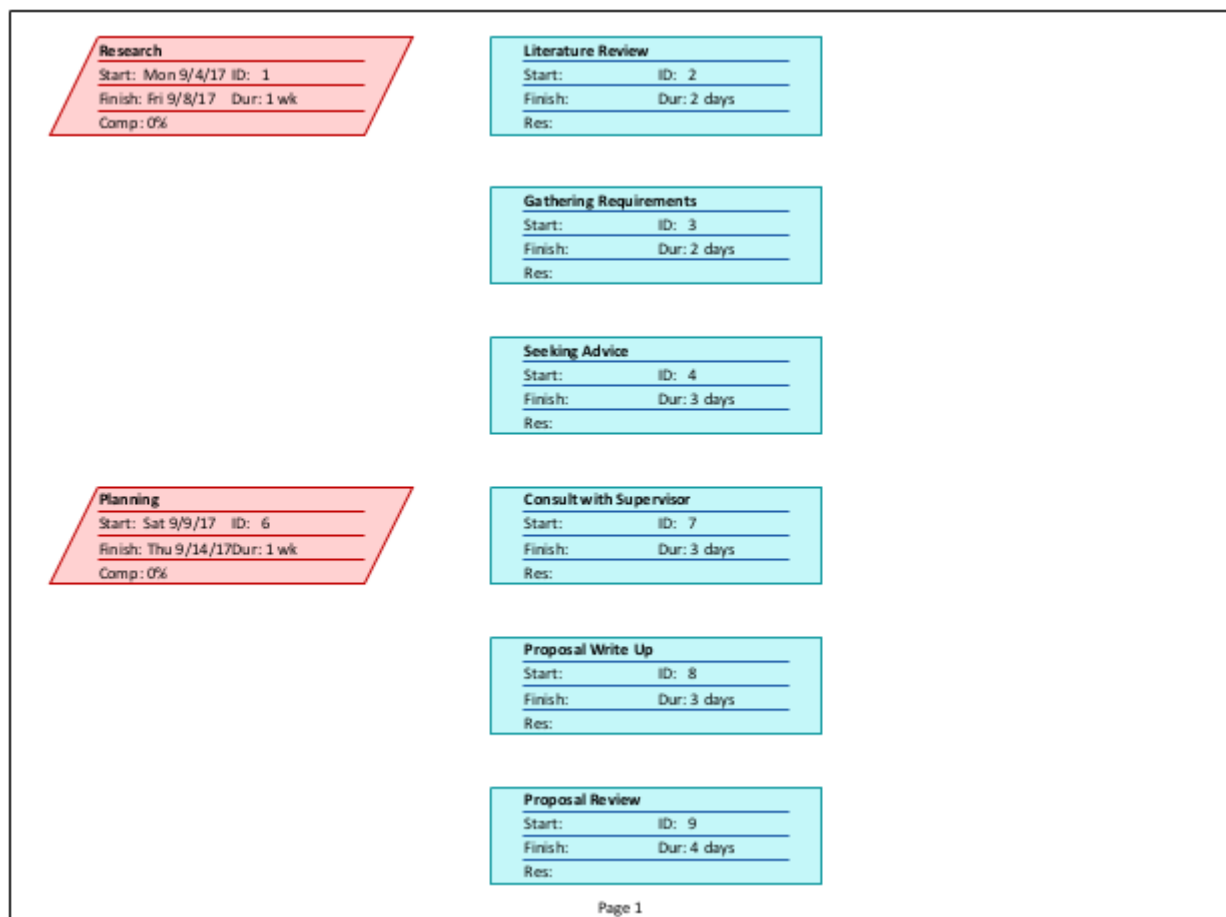
Project write up -

This is the documentation of the entire project.

Final project presentation –

The complete project is then presented on this date and the reports are then submitted

PROJECT MANAGEMENT NETWORK DIAGRAM



Analysis

Start: Fri 9/15/17 ID: 12
Finish: Thu 10/5/17 Dur: 3 wks
Comp: 0%

Gathering Requirements

Start: ID: 10
Finish: Dur: 4 days
Res:

Functional Requirements

Start: ID: 13
Finish: Dur: 1 wk
Res:

Feasibility Study

Start: ID: 14
Finish: Dur: 6 days
Res:

Consult with Supervisor

Start: ID: 15
Finish: Dur: 1 day
Res:

Evaluation

Start: ID: 16
Finish: Dur: 6 days
Res:

Verification

Start: ID: 17
Finish: Dur: 5 days
Res:

Validation

Start: ID: 18
Finish: Dur: 2 days
Res:

Design

Start: Fri 10/6/17 ID: 20
Finish: Thu 10/26/17 Dur: 3 wks
Comp: 0%

Use Cases

Start: ID: 21
Finish: Dur: 1 wk
Res:

Data Flow Diagrams

Start: ID: 22
Finish: Dur: 5 days
Res:

Entity Relationship Diagrams

Start: ID: 23
Finish: Dur: 5 days
Res:

Flow Charts

Start: ID: 24
Finish: Dur: 3 days
Res:

Consult with Supervisor

Start: ID: 25
Finish: Dur: 1 day
Res:

Start:	ID: 26
Finish:	Dur:
Res:	

Implementation	
Start: Fri 10/27/17	ID: 27
Finish: Thu 11/23/17	Dur: 4 wks
Comp: 0%	

Interfacing the webcam module with I	
Start:	ID: 28
Finish:	Dur: 1 wk
Res:	

configuring the graylog webserver	
Start:	ID: 29
Finish:	Dur: 1 wk
Res:	

configuring the wifi adapters and host	
Start:	ID: 30
Finish:	Dur: 1 wk
Res:	

configuring the router and firewall	
Start:	ID: 31
Finish:	Dur: 5 days
Res:	

Consult with Supervisor	
Start:	ID: 32
Finish:	Dur: 1 day
Res:	

Prototype Presentation	
Start:	ID: 33
Finish:	Dur: 1 day
Res:	

Start:	ID: 34
Finish:	Dur:
Res:	

Report write up	
Start:	ID: 35
Finish:	Dur: 1 wk
Res:	

CHAPTER 6: DESIGN.

This chapter will cover the major decisions which were undertaken while designing the system. Here we will take a look at the systems designs and components while describing each functionality and how they work together with the web interface.

The user interface has two use cases, a normal user and an admin. Below are the use-case diagrams, flowcharts, Data flow diagrams and entity relationship diagram that guided me in the implementation of the system.

6.1 USE-CASE DIAGRAM

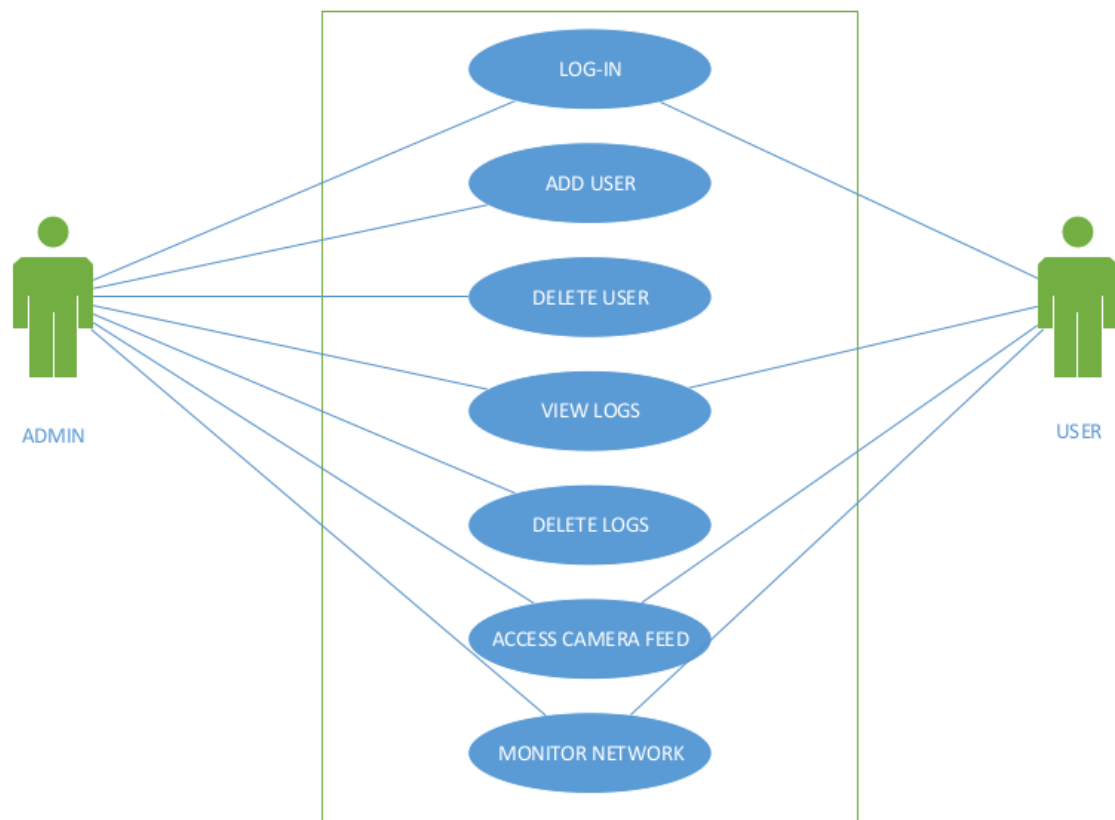


Fig 6. use-case diagram

In the use case diagram, there are two users an admin and a user, where a user has several enabled functionalities like login, view logs, access camera feed and monitor network, while the admin can perform all the functionalities the user is able to do and also add a user, delete a user and delete file logs.

6.2 ENTITY RELATIONSHIP DIAGRAM

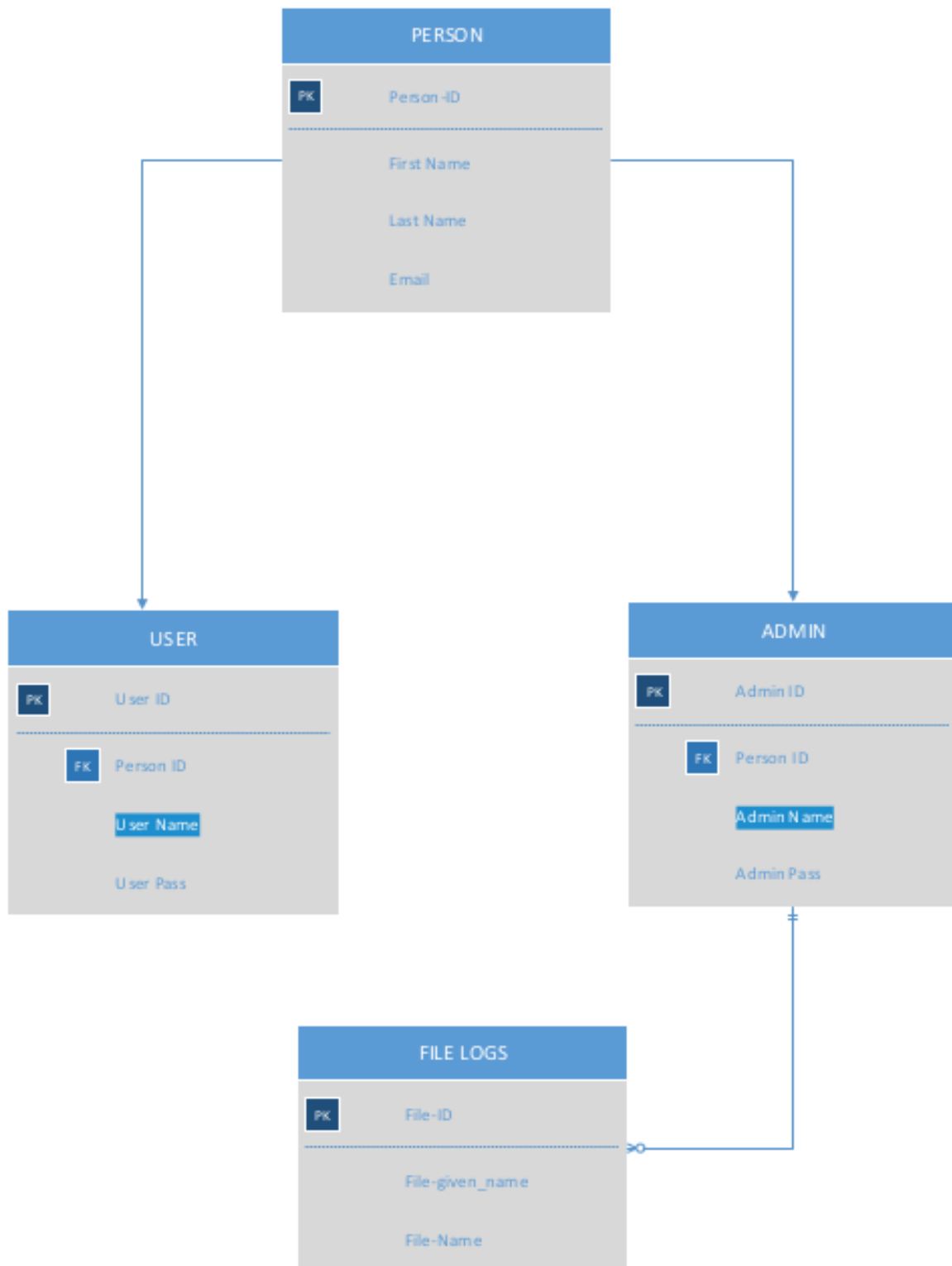


Fig 7. entity relationship diagram

The entity diagram describes how my database is, where I have one main database with three entities, user and admin entity where they inherit attributes from the person entity. We also have the admin entity where it has a one and only one to many relationship with the file log entity where only one and only one admin can access zero to many file log entity.

6.3 DATA FLOW DIAGRAM

6.3.1 USER:

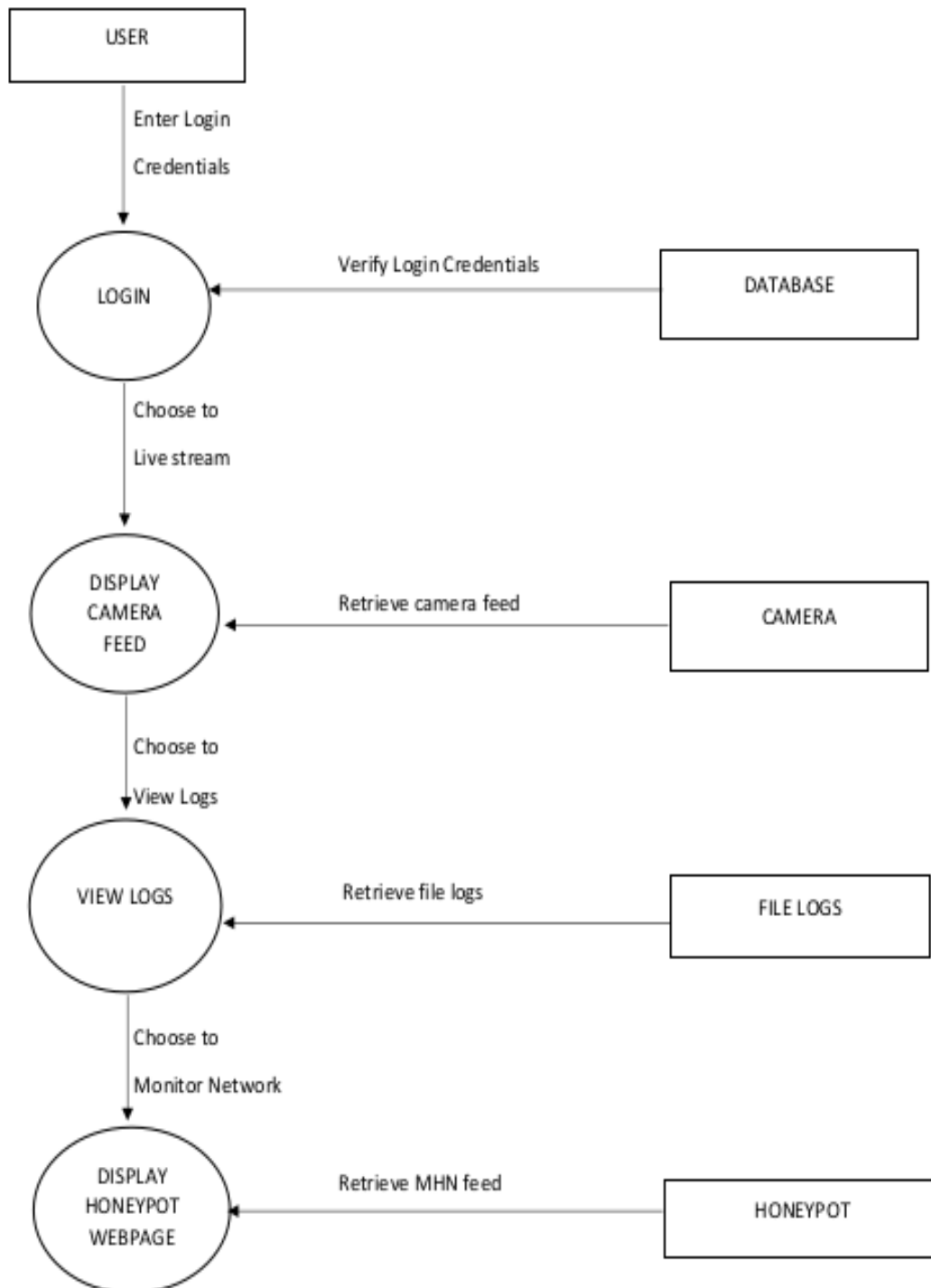


Fig 8. user data flow diagram

The user data flow diagram shows how the data flows in the system when a user access the system, where the user is first prompted to login then the system verifies login credentials, then he/she is prompted to choose a functionality display camera feed, where the system retrieves the camera feed from the host, view logs retrieves active directory file logs from the host and if it is display network monitoring webpage the system retrieves the network data output page.

6.3.2 ADMIN:

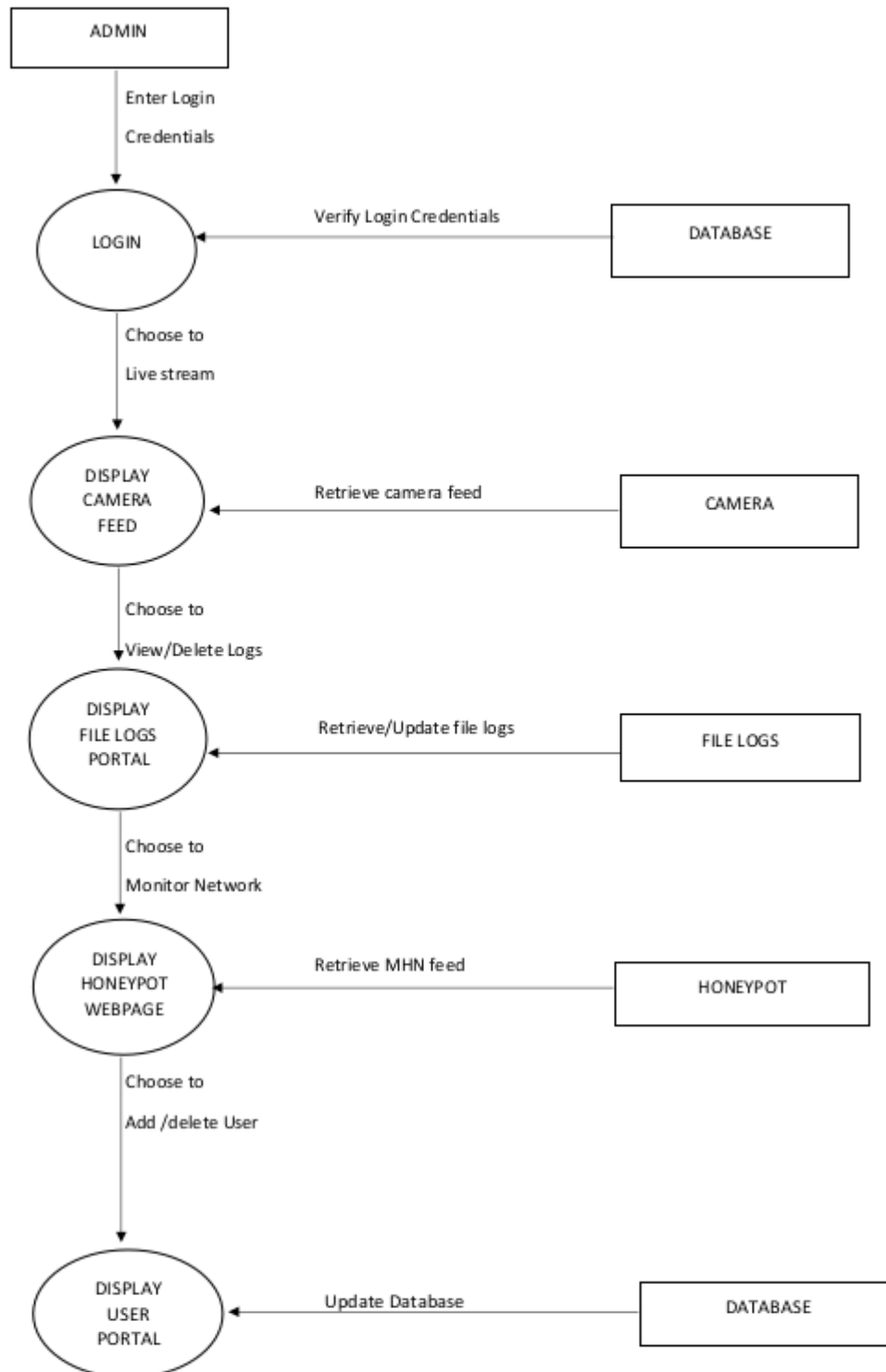


Fig 9. admin data flow diagram

The admin data flow diagram shows how the data flows in the system when the admin access the system, the diagram works the same as for the user but has added functionality of displaying user portal and backup portal (the backup portal functionality came as a last minute implementation of the system).

6.4 FLOW CHART

6.4.1 USER:

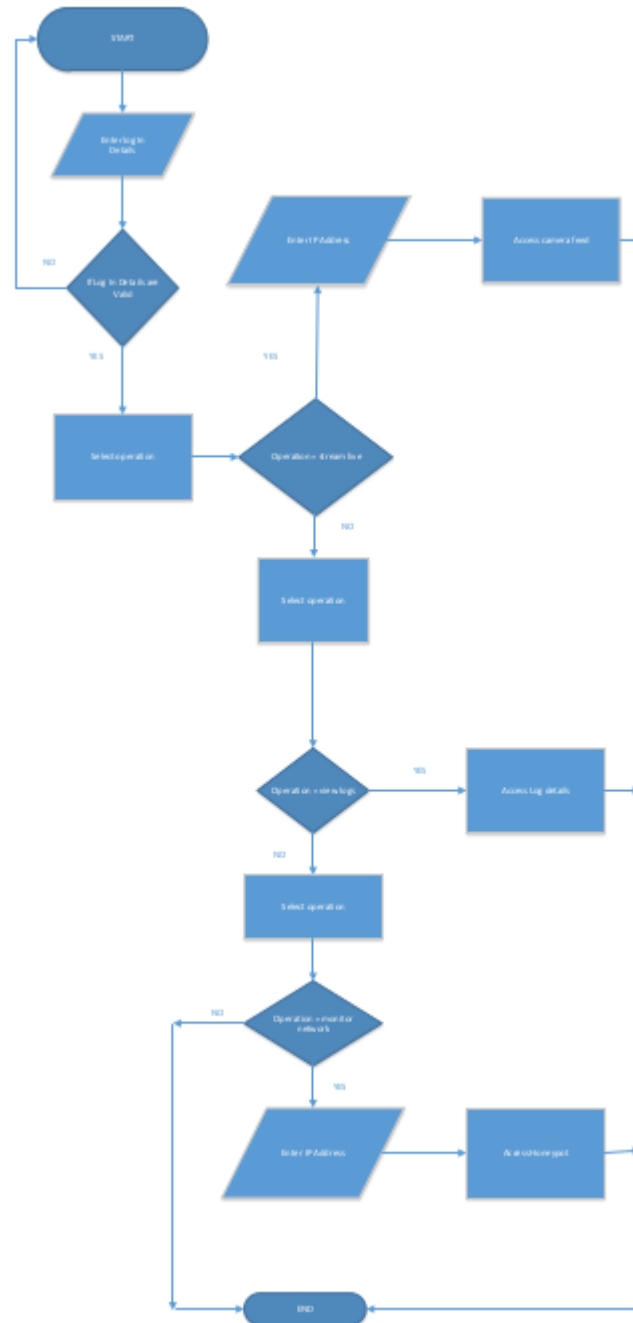


Fig 10. user flowchart

The user flow chart flow chart shows how the system flow is from the users side from the start from login through each functionalities if selected or not selected showing scenarios of each choice made till the end of the system process.

6.4.2 ADMIN:

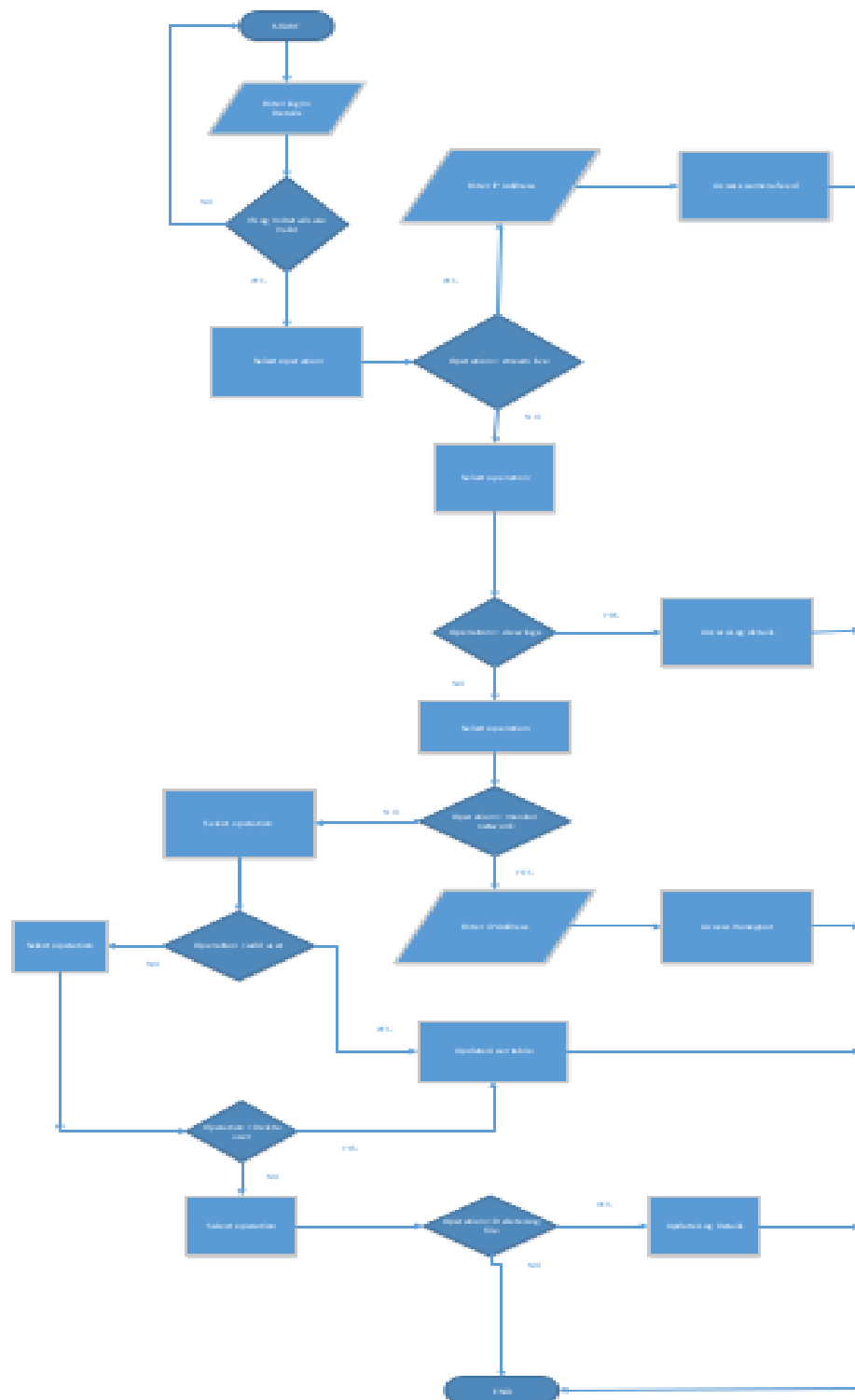


Fig 11. admin flowchart

The admin flowchart goes in the same context as the user flow chart but in the admin flow chart there is presence of more added functionalities in the system.

I would like to comment on some changes that were made during the end of the implementation stage that was not encountered during the design phase, for the network monitoring the system that I had planned to provide that functionality gave me some errors during configuration which is the honeypot and due to time during the implementation phase I had to set up a different tool that I will explain on the next chapter, but it should be noted both systems working together for network monitoring is possible and can be implemented in the future.

CHAPTER 7: IMPLEMENTATION.

The main aim of this chapter is to explain how my home surveillance and network monitoring system was developed as well as including snippets of codes, languages used and tools used to finish the system.

7.1 THE SURVEILLANCE MONITORING SYSTEM

The surveillance system consist of the main components that were listed in the requirements list. All the components were assembled on a workbench before packaging. The components for the surveillance system were; USB webcam, WiFi adapter and power cable with the power supply.

Then the programs run in the RPi. The program performing the surveillance system is known as motion and below I will explain the fundamental areas that allow the system to work.

So for the program to work with the camera, there are a few things that need to be defined in the configuration file where they differ according to the camera being used.

The webcam that I was working with was a logitech c270 HD webcam.

7.1.1 CAMERA SPECS

These are the specs that will be needed to be defined in the configuration file:

Image capture(4:3 SD) :

320 * 240, 640 * 480, 800 * 600

Image capture(16:9 W) :

360p, 480p, 720p

Frame Rate (max):

30fps @ 640 * 480



Fig 12. logitech c270 webcam

Fig 12. logitech webcam

The program needs to be directed on which camera device to use and below is how the program has been directed to the device. The host has been installed a raspbian OS where it is a UNIX system. When a USB device is usually plugged in a UNIX system the device is usually mounted on the device directory.

Then one needs to specify the max frame rate of the webcam, frame rate is the frequency at which consecutive images called frames are displayed in an animated display.

```
pi@raspberrypi:~ $ ls /dev
autofs          loop1          null           rfkill         tty21          tty41          tty61          vcs7
block           loop2          ppp            serial0        tty22          tty42          tty62          vcsa
btrfs-control  loop3          ptmx           shm            tty23          tty43          tty63          vcsa1
bus            loop4          pts            snd            tty24          tty44          tty7           vcsa2
cachefiles     loop5          ram0           stderr         tty25          tty45          tty8           vcsa3
char           loop6          ram1           stdin          tty26          tty46          tty9           vcsa4
console        loop7          ram10          stdout         tty27          tty47          ttyAMA0        vcsa5
cpu_dma_latency loop-control   ram11          tty            tty28          tty48          ttyprintk      vcsa6
cuse           mapper        ram12          tty0           tty29          tty49          uhid            vcsa7
disk           media0        ram13          tty1           tty3           tty5           uinput         vcsn
fb0            mem           ram14          tty10          tty30          tty50          urandom        vchi
fd             memory_bandwidth ram15          tty11          tty31          tty51          v4l            video0
full           mmcblk0        ram2           tty12          tty32          tty52          vchiq          watchdog
fuse           mmcblk0p1      ram3           tty13          tty33          tty53          vcio            watchdog0
gpiochip0      mmcblk0p2      ram4           tty14          tty34          tty54          vc-mem         zero
gpiomem        mmcblk0p5      ram5           tty15          tty35          tty55          vcs
hwrng          mmcblk0p6      ram6           tty16          tty36          tty56          vcs1
initctl        mmcblk0p7      ram7           tty17          tty37          tty57          vcs2
input          mqueue         ram8           tty18          tty38          tty58          vcs3
kmsg           net            ram9           tty19          tty39          tty59          vcs4
log            network_latency random          tty2           tty4           tty6           vcs5
loop0          network_throughput raw             tty20          tty40          tty60          vcs6
```

Fig 13. device directory listing on my host.

```
#####
[?] Capture device options
#####
# Videodevice to be used for capturing (default /dev/video0)
videodevice /dev/video0
```

Fig 14. camera access path to directory

```
# Maximum number of frames to be captured per second.
# Valid range: 2-100. Default: 100 (almost no limit).
framerate 30
```

Fig 15. camera frame rate

This is where we define the stream display size during streaming, where width has been set to 800 pixels and height 600 pixels. Then we define the storage path when motion is detected it stores the images and snap videos of 30 seconds length.

```
# Image width (pixels). Valid range: Camera dependent, default: 352
width 800

# Image height (pixels). Valid range: Camera dependent, default: 288
height 600
```

Fig 16. camera Image capture

```
# Target base directory for pictures and films
# Recommended to use absolute path. (Default: current working directory)
target_dir /home/pi/project/webcam-images
```

Fig 17. target directory that stores the images and videos while captured

This is where we define the listening stream port and authentication syntax when accessing the live stream feed.

```
#####
# Live Stream Server
#####

# The mini-http server listens to this port for requests (default: 0 = disabled)
stream_port 9080
```

Fig 18. Stream port number

```
# Authentication for the stream. Syntax username:password
# Default: not defined (Disabled)
; stream_authentication pi:ra5p!E
```

Fig 19. Stream authentication

7.2 THE NETWORK MONITORING SYSTEM

During implementation of the network monitoring system I had planned to install a low interactive honeypot for monitoring the network.

A honeypot is basically a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. (honeypot, wikipedia).

To better understand the value of honeypots, we can break them down into two different categories: production and research. Production honeypots are used to protect your network, they directly help secure your organization. Research honeypots are different; they are used to collect information. That information can then be used for a variety of purposes, such as early warning and prediction, intelligence gathering, or law enforcement.(honeyd, symantec)

My aim was to deploy a production honeypot, where the honeypot is a honeyd. It was created and maintained by Niels Provos. It's designed to be used on Unix-based operating systems, such as OpenBSD or Linux; however, it can also be used on a Windows operating system. Since this solution is OpenSource, not only is it free, but we also have full access to the source code, which is under the BSD license (honeyd, symantec).

With all these said I was unable to deploy the honeypot, and due to time I had to look for another way to attain that main functionality of network monitoring. After going back to my books I remembered I was reading some post on another tool known as nzyme a WiFi Monitoring, Intrusion Detection and Forensics tool that was released on October 2nd 2017 by Lennart Koopmann. The tool basically uses a WiFi adapter in monitor mode to sniff management frames from all configured 2.4Ghz or 5Ghz channels and writes them into a graylog instance for monitoring and analysis(nzyme, wtf.horse).

So the components used for network monitoring was a WiFi adapter with monitor mode capabilities connected to the host system.

After setting up the graylog web server on my machine I started a global input which allows the nzyme tool on the RPi host system to send the frames to the graylog instance for analysis and monitoring.

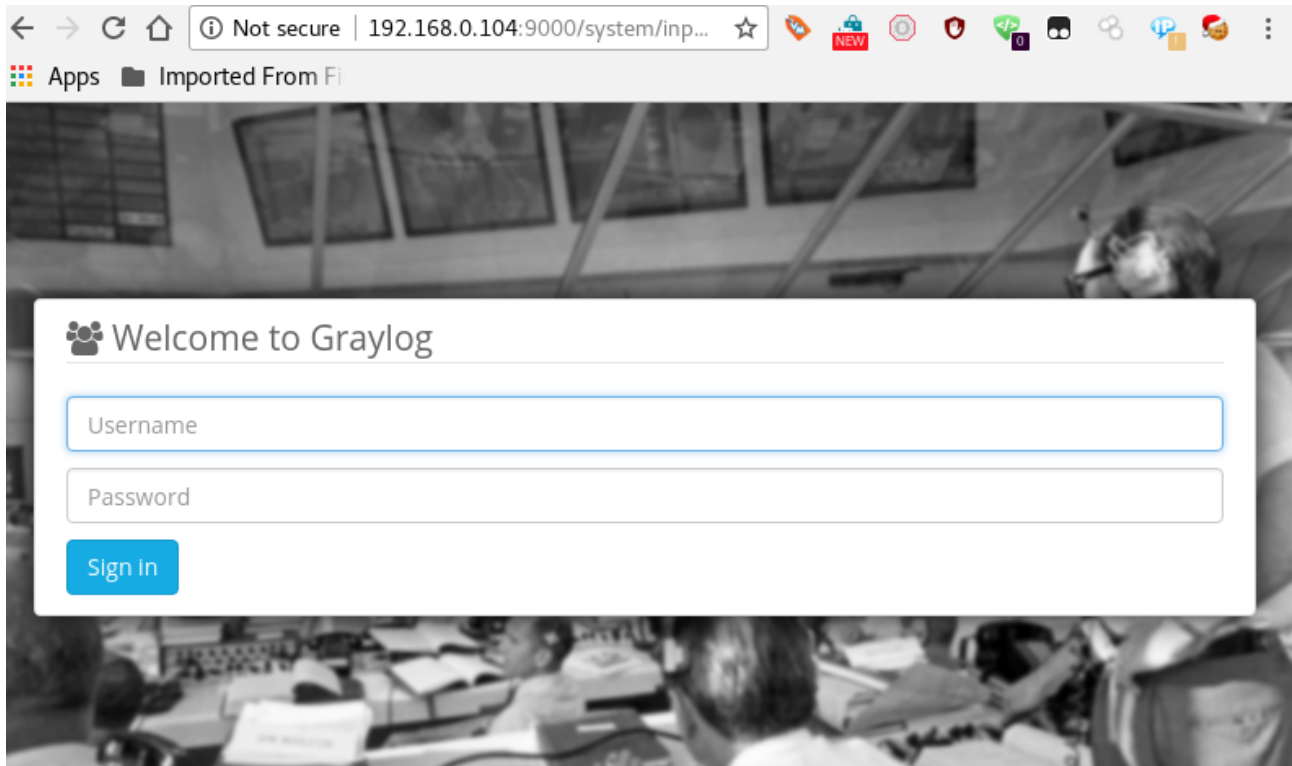


Fig 20. graylog web interface

The Nzyme input instance was a GELF TCP where it had a bind_address this works if the tool is running on the same host where the graylog open log management server has been installed, the override_source and port is where the nzyme can connect to the graylog host over the internet.

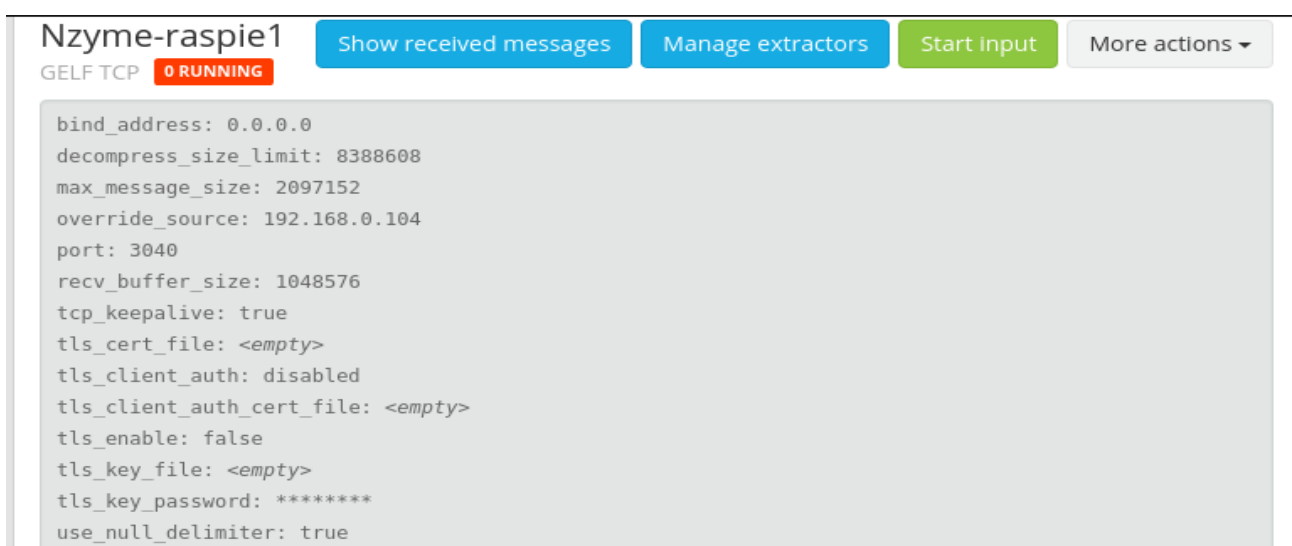


Fig 21. Gelf TCP global input for nzyme instance

This is the configuration of the nzyme-instance, where we configure the channels the WiFi adapter can hop on for sniffing and define the adapters name, the channel hop command is the instance where the adapter starts to hop on each channel on one interval with root access. The graylog_address is the connection path where the instance sends the sniffed frames from the RPi host to my host system.

```
# A name for this nzyme-instance.
nzyme_id = nzyme-sensor-1

# WiFi interface and 802.11 channels to use. Nzyme will cycle your network adapters through these channels.
# Consider local legal requirements and regulations. Default is US 2.4GHz band.
# Configure one or more interfaces here.
# See also: https://en.wikipedia.org/wiki/List_of_WLAN_channels
channels = wlan1mon:1,2,3,4,5,6,7,8,9,10,11,12,13,14

# There is no way for nzyme to configure your wifi interface directly. We are using direct operating system commands to
# configure the adapter. Examples for Linux and OSX are in the README.
channel_hop_command = sudo /sbin/iwconfig {interface} channel {channel}

# Channel hop interval in seconds. Leave at default if you don't know what this is.
channel_hop_interval = 1

# List of Graylog GELF TCP inputs. You can send to multiple, comma separated, Graylog servers if you want.
graylog_addresses = 192.168.0.104:3040
```

Fig 22. nzyme-instance config file on the RPi host

7.3 WEB INTERFACE

The web interface is used to perform the main functionalities the system provide. I used w3css, php, html and bootstrap to design and develop it. Because of the systems ability to access the internet I thought of the user interface being a web application. The web application runs along with an SQL database where it will be accessible over the internet.

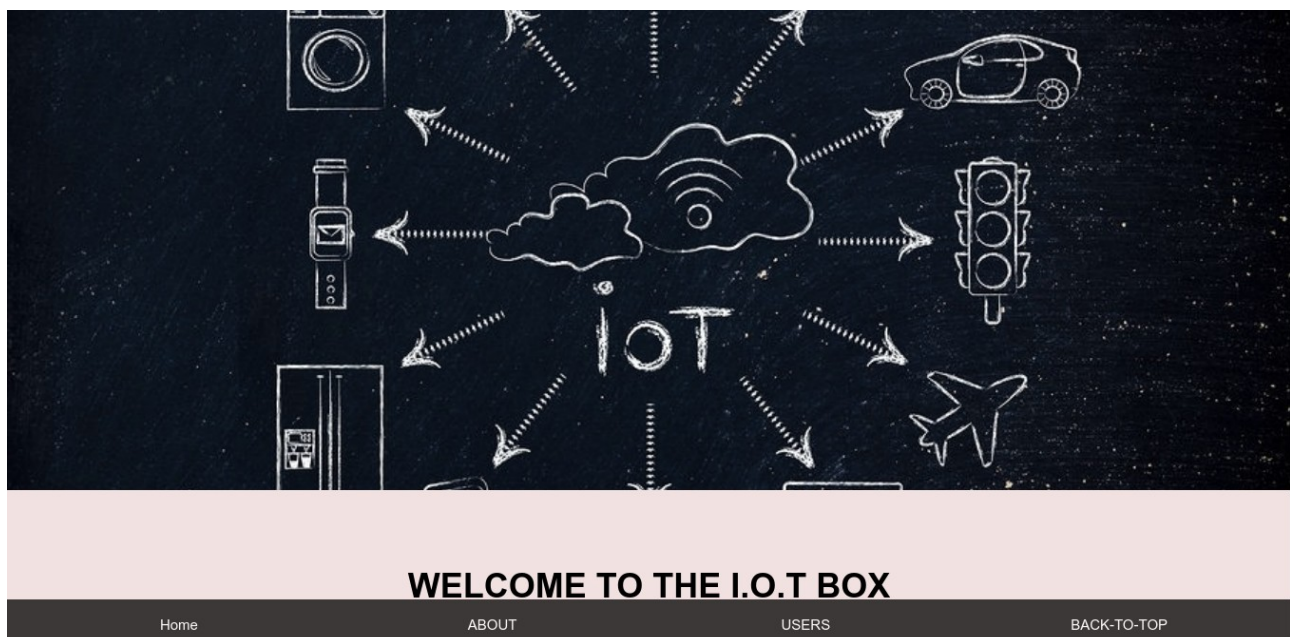


Fig 23. web interface welcome_page(a)

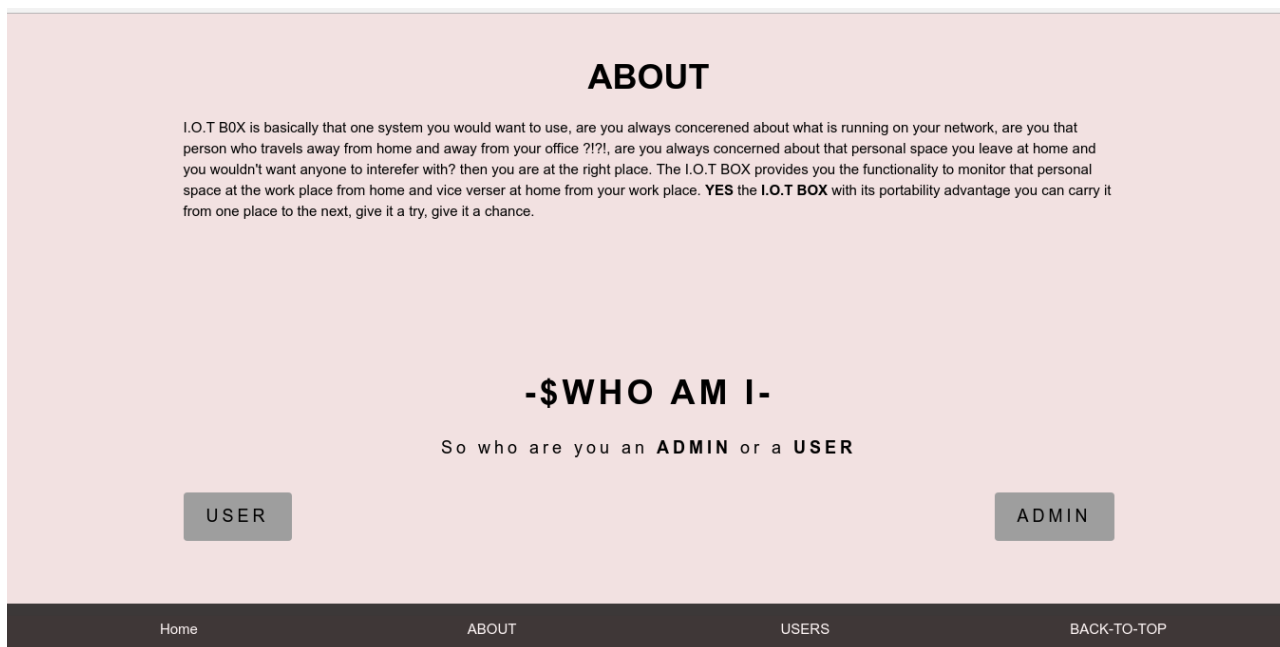


Fig 24. web interface welcome_page(b)

Welcome_Page of the website contains less information about the system as a security protocol. This is the starting line of my web interface.

7.3.1 USER WEB INTERFACE



Fig 25. user login interface prompt

The login prompt for the user when he/she clicks the user button on the users page on the Welcome_Page.php.

Below is a snippet of code on the login page where security implementation from SQL injections has been enforced.

There is also a simple security measure that has been enforced which is the error output given when the credentials of the login are wrong. It doesn't specify if either the password or the user email is wrong but gives you an invalid login details error output. I would say this is a security feature because before a hacker starts to attempt to crack your login

details using brute forcing technique he/she would attempt to put common known passwords like admin and 12345 if it gives him an error like invalid user pass, on would have given him some clue on where to start to attack your login page.

```
//preventing sql injection
$user_email= strip_tags($ POST['user_email']);
$user_pass= strip_tags($ POST['user_pass']);

        $user_email=stripslashes($user_email);
        $user_pass=stripslashes($user_pass);

$user_email=mysqli_real_escape_string($connection,$user_email);
$user_pass=mysqli_real_escape_string($connection,$user_pass);

$check_user="SELECT * FROM users_login WHERE user_email='$user_email'AND user_pass='$user_pass' LIMIT 1";

$run=mysqli_query($connection,$check_user);
$row=mysqli_num_rows($run);

if($row == 1)
{
    $_SESSION['user_email']=$user_email;
    $_SESSION['success']=$user_email;

    header("Location: Home_User.php");
}
else
{
    $error_msg = "INVALID LOGIN DETAILS Please try Again";
    header(("Location:User_Login.php? msg=$error_msg"));
}
```

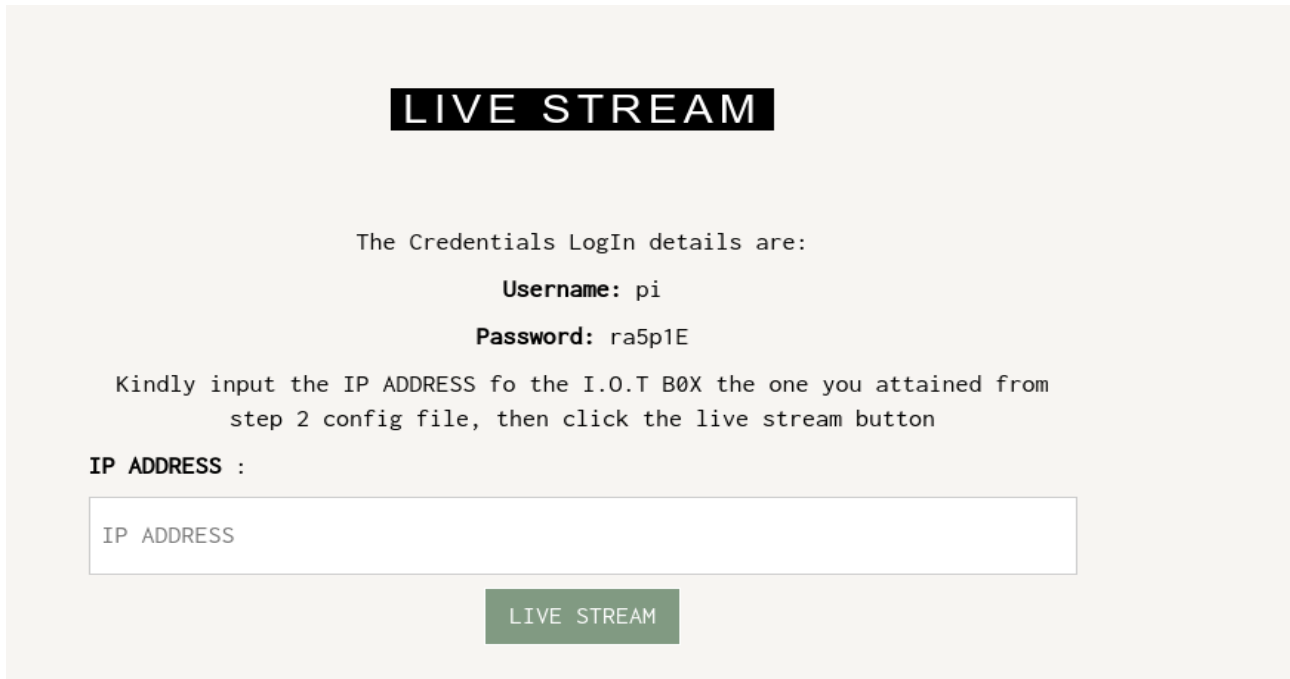
Fig 26. user login code

After the user has logged in he/she is forwarded to this page that contains the main functionalities of the system, the network monitoring and surveillance functionality.



Fig 27. users home page

The live stream functionality are actually the same for both users (admin and normal user), the user actually only needs an IP address to access the camera feed. In figure 29 the snippet image of the code explain how it access the camera feed from the system where on click of live stream button a new page address is open where it is http:// (the ip address submitted) :9080 and the port number which are the live server server (figure 18) configuration placed while setting up the surveillance system.



LIVE STREAM

The Credentials LogIn details are:

Username: pi

Password: ra5p1E

Kindly input the IP ADDRESS fo the I.O.T B0X the one you attained from
step 2 config file, then click the live stream button

IP ADDRESS :

IP ADDRESS

LIVE STREAM

Fig 28. live stream functionality

```

<h2 class="w3-center w3-padding-64"><span class="w3-tag w3-wide">LIVE STREAM</span></h2>

<center><p>The Credentials LogIn details are:</p></center>
<center><p><strong>Username:</strong> pi</p></center>
<center><p><strong>Password:</strong> ra5p1E</p></center>

<center><p>Kindly input the IP ADDRESS fo the I.O.T B0X the one you attained from step 2 config file, then
click the live stream button</p></center>

<p><strong>IP ADDRESS</strong> :</p>
<form>
  <p><input class="w3-input w3-padding-16 w3-border" type="text" placeholder="IP ADDRESS" id="ip_address_1"></p>
  <center><p><button class="w3-button w3-green w3-border w3-border-white" type="submit" name="livestream" onclick
="process()">LIVE STREAM</button></p></center>
</form>

<!--Live stream button function Script-->
<script>

function process(){
  var address = document.getElementById("ip_address_1").value;
  var url = "http://" + address + ":9080";
window.open(url);}

  </script>
</div>
</script>
</div>

```

Fig 29. live stream code

For the network monitoring functionality as I had said I was unable to deploy my honeypot which then I thought of this other tool for WiFi monitoring, in this functionality it is a button that the user clicks and opens a new page to the graylog web server where he/she will be prompted to input login credentials which are provided at the web interface, figure 31 explains how the code works where the graylog webserver listens on a certain url (http://ipaddress:portnumber or http://localhost:portnumber), for me as I was setting up my graylog webserver I set the listening url as my assigned ip address and the default port number which is http://192.168.0.104:9000. When the user click onto the graylog webserver button it directly opens a new page with the url http://192.168.0.104:9000.

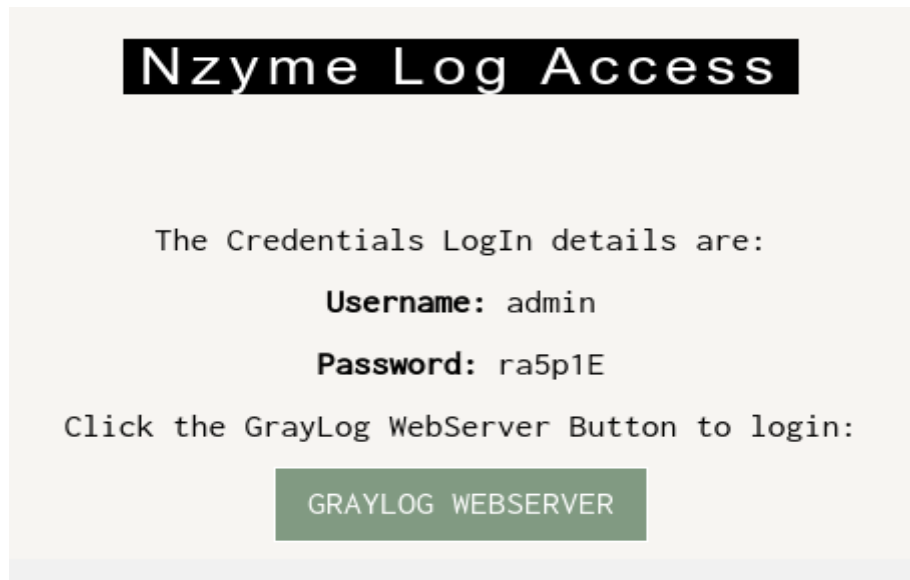


Fig 30. Nzyme log access

```
<div class="w3-container">
  <h2 class="w3-center w3-padding-64"><span class="w3-tag w3-wide">Nzyme Log Access</span></h2>

  <center><p>The Credentials LogIn details are:</p></center>
  <center><p><strong>Username:</strong> admin</p></center>
  <center><p><strong>Password:</strong> ra5p1E</p></center>

  <center><p>Click the GrayLog WebServer Button to login:</p></center>
  <center><p><button class="w3-button w3-green w3-border w3-border-white" type="submit" name="WebServer" onclick="
    process2()">GRAYLOG WEBSERVER</button></p></center>

  <!--Graylog WebServer button function Script-->
  <script>
    function process2(){
      var url1 = "http://192.168.0.104:9000";
      window.open(url1);}
  </script>
</div>
```

Fig 31. Nzyme log access code

For the other functionality the users have to view the real time logs when new motion is detected and an image and video time lapse of 30sec is captured and stored in the target directory (figure 17).

On the view logs code figure it basically explains how a user can access the real time logs, I was able to achieve this functionality by starting the simpleHTTPServer on the target directory. Where the url access will be the assigned ip address for the RPi host and port number 8000.

VIEW LOGS

Real Time Logs:

ACTIVE DIRECTORY

Fig 32. View Logs

```
</div>
<div class="w3-container" id="logs">
  <h2 class="w3-center w3-padding-64"><span class="w3-tag w3-wide">VIEW LOGS</span></h2>
  <center><p>Real Time Logs:</p></center>
  <center><p><button class="w3-button w3-green w3-border w3-border-white" type="submit" name="WebServer" onclick="
    process3()">ACTIVE DIRECTORY</button></p></center>

<!--Graylog WebServer button function Script-->
  <script>
    function process3(){
      var url1 = "http://192.168.0.100:8000";
      window.open(url1);}
  </script>
</div>
```

Fig 33. View Logs codes

7.3.2 ADMIN WEB INTERFACE

The admin interface is almost the same for the user interface though I am going to show case the added functionalities the admin has. The configuration files is not a functionality but they are guides that will help the admin to setting up the system and start running it.

CONFIG FILES

Dear Admin Here are the files for setting up the **I.O.T BOX ??** to get started to using it !!

[*STEP-1*](#)

[*STEP-4*](#)

[*STEP-2*](#)

[*STEP-5*](#)


[*STEP-3*](#)

[*STEP-6*](#)

You are **STRONGLY ADVISED** these configuration files guide you to set up your I.O.T BOX to **!!DEFAULT SETTINGS!!**, for security purposes while setting up the I.O.T BOX **CHANGE** the **!!default settings!!**


Fig 34. Configuration files

The admin interface has two more added functionalities, Users Portal, where it is the portal for the admin to manage users, by manage is add and delete users and the Back Up portal where it is the portal for the admin to manage the file captured by the camera, at this section the admin has a user guide for file transfer from the RPi host to the host machine where he/she can upload the files. At this portal the uploaded files are usually listed and the admin has the ability to delete listed files.



-USERS PORTAL-

-REGISTERED USERS-




USER ID	USER NAME	USER E-MAIL	
1	pnumi	pnumi@homesys.com	<div>Delete</div>
2	sir	sir@homesys.com	<div>Delete</div>
3	pete	pete@homesys.com	<div>Delete</div>

Fig 35. users portal (registered users)

-USERS PORTAL-

-ADD USER-



USER DETAILS

USER NAME

EMAIL

PASSWORD

ADD USER

Fig 36. users portal (Add user form)

User Name	User Email
pnumi	pnumi@homesys.com
Are you sure you want to delete this record?	
Delete	Cancel

Fig 37. users portal (deleting user output)

-BACKUP PORTAL-

Name	Image	
testing 4		Delete
test		Delete
two-two		Delete
try-error		Delete
length skip		Delete
center		Delete


"Before you head on, to back up your active directory logs, have you retrieved them from your **LO.T BOX**? I you have go on ahead to Backing up your files and enjoy if not dear ADMIN click **HERE** and follow the steps enjoy!!"

By: Backup-Buddy :)

Fig 38. backup portal (uploaded files listing)

-BACKUP PORTAL-

-BACKUP FILE-



BACKUP DETAILS

FILE NAME:

FILE: No file chosen

Fig 39. backup portal (upload file)


Name	Image
testing 4	
Are you sure you want to delete this record?	
<input type="button" value="Delete"/>	<input type="button" value="Cancel"/>

Fig 40. backup portal (deleting file output)

7.4 INTERNET CONNECTION

For the internet connection the component at work was the router, so basically I had to configure the router to allow access of the system through the internet. I performed several task:

- a) reserving ip address for all components connected to the internet, one can also set static IP addresses on your RPi host system if you do not have a router.
- b) allowed port forwarding rules on the router.
- c) Set firewall rules on my host system using IP TABLES

Iptables is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on your system, iptables looks for a rule in its list to match it to. If it doesn't find one, it resorts to the default action.

TP-LINK 150Mbps Wireless N Router Model No. TL-WR720N

Address Reservation

ID	MAC Address	Reserved IP Address	Status	Modify
1			Enabled	Modify Delete
2			Enabled	Modify Delete
3			Enabled	Modify Delete
4			Enabled	Modify Delete

[Add New...](#) [Enable All](#) [Disable All](#) [Delete All](#)

[Previous](#) [Next](#)

Address Reservation Help

When you specify a reserved IP address for a PC in the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses could be assigned to servers that require permanent IP settings.

- **MAC Address** - The MAC Address of the PC that you want to reserve an IP address for.
- **Reserved IP Address** - The IP address that the Router reserved.
- **Status** - It shows whether the entry is enabled or not.
- **Modify** - To modify or delete an existing entry.

To Reserve IP Addresses, you can follow these steps:

1. Enter the MAC Address (The format for the MAC Address is XX-XX-XX-XX-XX-XX) and the IP address in dotted decimal notation of the computer you wish to add.
2. Click the **Save** button.

To modify a Reserved IP Address, you can follow these steps:

1. Select the reserved address entry as you desired, modify it. If you wish to delete the entry, click the **Delete** link of the entry.
2. Click the **Save** button.

Click the **Add New...** button to add a new Address Reservation entry.

Click the **Enable All** button to enable all the entries in the table.

Click the **Disable All** button to disable all the entries in the table.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Note: The changes will not take effect until the Router reboots.

*Click Add New

Add or Modify an Address Reservation Entry

Fig 41. IP reservation on router

Virtual Servers

ID	Service Ports	IP Address	Protocol	Status	Modify
1	9080	192.168.0.100	TCP	Enabled	Modify Delete
2	9080	192.168.0.100	UDP	Enabled	Modify Delete

Add New...

Enable All

Disable All

Delete All

Fig 42. port forwarding rules enabling on router

Port Triggering						
ID	Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status	Modify
1	9080	ALL	8080-9080	ALL	Enabled	Modify Delete
<div><button>Add New...</button><button>Enable All</button><button>Disable All</button><button>Delete All</button></div>						

Fig 43. port triggering rules enabling on router

```
root@gr00t:/home/g3k1e# sudo /sbin/iptables-save
# Generated by iptables-save v1.6.1 on Fri Dec 8 08:54:06 2017
*filter
:INPUT ACCEPT [2925:1020123]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [2818:681279]
COMMIT
# Completed on Fri Dec 8 08:54:06 2017
```

Fig 44. IP tables configured rules.

CHAPTER 8: CHALLENGES.

The project had 3 main challenges ;

8.1 LOW END DEVICES.

This was a great challenge that I met and had to make me find other ways of making the system work despite the challenge. Low end devices mean low processing power and low quality output of the system.

8.2 COST.

This was also a major challenge I faced because for a great system one has to meet requirements of high end devices, for my project me being a student cost was one thing I was trying to avoid and make the project less cost effective, but if the project is to be manufactured and build at a great scale the cost would be less effective because the requirements needed would be bought in bulk, but for a small system manufacturing at a small scale production the cost would vary on the type of components being bought and used.

8.3 HONEYPOT DEPLOYMENT.

This was also a major challenge I faced because honeypots deployments require knowledge of what type of honeypot you require its main objective then its configuration and build. The challenge I faced was building or rather would I say installing the honeypot system in the RPi host, this being a challenge because I was being rather conscious of not breaking my whole system, however I overcame this challenging by installing the nzyme tool which met the network monitoring functionality.

CHAPTER 9: EVALUATION.

This chapter explains the and shows the test results undertaken on the system.

The testing process will test the two main functionalities of the system which is the surveillance system and network monitoring system.

9.1 TEST: SURVEILLANCE AND NETWORK MONITORING SYSTEM COMPONENTS TEST

Components present:

- 1) WEBCAM
- 2) WiFi Adapters

9.1.2 WEBCAM TEST: Turn on webcam indicator.

How I conducted this test is by use of my terminal mode on my RPi host, by starting the program itself to see if the webcam will turn on.

```
pi@raspberrypi:~ $ sudo motion
[0:motion] [NTC] [ALL] conf_load: Processing thread 0 - config file /etc/motion/
motion.conf
[0:motion] [NTC] [ALL] motion_startup: Motion 4.0 Started
[0:motion] [NTC] [ALL] motion_startup: Logging to file (/var/log/motion/motion.l
og)
pi@raspberrypi:~ $ █
```

Fig 45. starting surveillance program.



Fig 46. Webcam led green indicator turned on

9.1.3 WiFi ADAPTERS TEST: Turn on webcam indicator.

How I conducted this test is by use of my terminal mode on my RPi host, by using command `iwconfig`, this command is a unix command that allows one to see wifi adapters present and their status.

```
pi@raspberrypi:~ $ iwconfig
wlan0 IEEE 802.11 ESSID:"GUEST's"
Mode:Managed Frequency:2.437 GHz Access Point: 62:E3:27:C1:AE:E0
Bit Rate=150 Mb/s Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:off
Link Quality=65/70 Signal level=-45 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:12 Invalid misc:252 Missed beacon:0

lo no wireless extensions.

eth0 no wireless extensions.

wlan1 IEEE 802.11 ESSID:"GUEST's"
Mode:Managed Frequency:2.437 GHz Access Point: 62:E3:27:C1:AE:E0
Bit Rate=150 Mb/s Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:off
Link Quality=70/70 Signal level=-39 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:30 Missed beacon:0
```

Fig 47. present wifi adapters.

All the wifi adapters are present but now we have to turn one of the adapters in monitor mode which is the wlan1 adapter. I am going to use aircrack-ng commands which is already installed in the system.

```
pi@raspberrypi:~ $ sudo airmon-ng start wlan1

Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

PID Name
247 avahi-daemon
254 dhcpcd
255 avahi-daemon
474 wpa_supplicant
899 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 rt2800usb Ralink Technology, Corp. RT5370
phy1 wlan1 rtl8187 Realtek Semiconductor Corp. RTL8187

(mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
(mac80211 station mode vif disabled for [phy1]wlan1)
```

Fig 48. starting wlan1 wifi adapter to monitor mode.

When we issue the iwconfig command again we can see the adapter has been started to monitor mode.

```
pi@raspberrypi:~ $ iwconfig
wlan0 IEEE 802.11 ESSID:"GUEST's"
Mode:Managed Frequency:2.437 GHz Access Point: 62:E3:27:C1:AE:E0
Bit Rate=150 Mb/s Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:off
Link Quality=69/70 Signal level=-41 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:12 Invalid misc:286 Missed beacon:0

lo no wireless extensions.

eth0 no wireless extensions.

wlan1mon IEEE 802.11 Mode:Monitor Frequency:2.442 GHz Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:on
```

Fig 49. confirming wlan1 is in monitor mode.

TEST N.O	TEST NAME	EXPECTED RESULTS
<u>1</u>	Turn on the webcam light	Green light to turn on
<u>2</u>	Test WiFi Adapters	One WiFi adapter to be on monitor mode the other connected to an WiFi Access Point

According to the table below the evaluation test was successful because we attained each expected results from our tests.

CHAPTER 10: CONCLUSION.

This chapter will focus on how the project was successful in comparison to the original aims and objectives. It also take part to add on what can be added in future and with more time and describing new skills attained through the project design and implementation.

So the main aims I originally had were:

- To provide user friendly user interface for accessing the system functionalities.
- Combine both network monitoring and surveillance monitoring in one whole system.
- Implement a portable system.

User friendly Is the system user friendly: I would say yes to this with the provided user guides for setting up the whole system, the user interface provides functionality to interact with the system without requiring more knowledge and skills of computer technology.

Combination of both network and surveillance system: yes this aim was achieved where both functionalities were met despite the honeypot deployment challenge.

Portability of the system: yes this objective was successfully achieved.

10.1 FUTURE WORK

The system can be implemented for greater use, where one can also add a gsm module on the RPi host so that when the internet goes down surveillance monitoring will still be active.

For security purposes with the deployment of honeypot, this will show if the any host machine is being targeted by an attacker, one can also use vpn connection to access the system so as to secure ones data streams from the system to the user interface.

REFERENCES

- Camera, T. S. (2015). *topsurveillancesystems.com*. Retrieved from Top Surveillance Camera: <https://www.topsurveillancesystems.com/>
- Cecil, A. (2006). *A Summary of Network Traffic Monitoring and Analysis Techniques*. Retrieved from Washington University in St.Louis: http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring.pdf
- Fingas, J. (2014). Stuxnet worm entered Iran's nuclear facilities through hacked suppliers. *cyberattack, cyberwarfare, duqu, energy, internet, iran, kaspersky, kasperskylab, KasperskyLabs, netlock, nuclear, nuclearpower, nuclearweapons, security, stuxnet*.
- Gus. (2015). *PiMyLifeUp*. Retrieved from pimylifeup.com: <https://pimylifeup.com/raspberry-pi-security-camera/>
- Kille, L. W., & Maximino, M. (11 February 2014). The effect of CCTV on public safety: Research roundup. *Harvard Kennedy School's Shorenstein Center and the Carnegie-Knight Initiative*.
- Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.
- openmaniak. (2010, December 10th). *wireshark_conf*. Retrieved from openmaniak.com: https://openmaniak.com/wireshark_conf.php
- wikipedia. (2016, February 8th). *History of surveillance*. Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/History_of_surveillance
- Wikipedia. (2017, August 28th). *Computer_and_network_surveillanc*. Retrieved from wikipedia.org: [**https://en.wikipedia.org/wiki/Computer_and_network_surveillance**](https://en.wikipedia.org/wiki/Computer_and_network_surveillance)

GLOSSARY

GSM - is a standard developed by the European Telecommunications Standards Institute to describe the protocols for second-generation digital cellular networks used by mobile devices such as tablets.

SQL - Structured Query Language (SQL) is a standard computer language for relational database management and data manipulation. (Structured Query Language (SQL))

RPi: Raspberry pi

CCTV – Closed-Circuit Television, also known as video surveillance.

RFID - Radio-frequency identification uses electromagnetic fields to automatically identify and track tags attached to objects.

GPS - Global Positioning System, originally Navstar GPS, is a space-based radio navigation system.