CENTRALIZED HUB FOR SECURING A NETWORK OF IoT DEVICES

2020-086

Project Proposal Report

IT 17009614 – Abeykoon A.M.I.S

Bachelor of Science (Hons) Degree in Information Technology
Specialized in Cyber Security

Department of Information Systems Engineering

Sri Lanka Institute of Information Technology
Sri Lanka

February 2020

CENTRALIZED HUB FOR SECURING A NETWORK OF IoT DEVICES

2020-086

Project Proposal Report

Bachelor of Science (Hons) Degree in Information Technology
Specialized in Cyber Security

Department of Information Systems Engineering

Sri Lanka Institute of Information Technology
Sri Lanka

February 2020

DECLARATION

I declare that this is our own work and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID	Signature
A.M.I.S Abeykoon	IT 17009614	

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

Signature of the Supervisor: Date:

ABSTRACT

Internet of Things (IoT) devices connected to a specific network is accessed by the user through a home router where each device will be assigned a port individually and there will be no proper mechanism to authenticate if the user is legitimate or if it is an attacker trying to gain access to the devices by compromising the network. In case of a compromise, the whole network of devices can be taken down. When considering the information security, it can create different levels of impact based on the level of sensitivity of the information that the devices contain the information can be disclosed to unwanted/ unauthorized parties. Which can later be used for other purposes by them for financial means. Therefore, research is to implement plug and play (PnP) device 'ARCSECURE' to mitigate IoT security risk at small office, home office (SOHO) environment.

Most common attack to the IoT environment is botnets. Large number of IoT devices contains high computation power. Botnet use this computation power to crypto currency mining. The proposed solution is to mitigate botnet attacks implement Host-based intrusion prevention system (IPS) system. To detect intrusion, System is going to use anomaly based method and protocol based method. Anomaly based method use neural-network based intrusion-detection technique. Protocol based method use machine learning module.

Keywords: Machine Learning, Neural-network, Internet Security, Botnet

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

IoT	Internet of Things
SOHO	Small office Home office
PnP	Plug and Play
IPS	Intrusion preventions system
IDS	Intrusion detection system
DDoS	Distributed denial of service
RBFN	Radial basis-function networks

1 INTRODUCTION

1.1 Purpose

Internet of things (IoT) connects the digital world with the living world. This connection establishes with network of distributed (sensor) nodes, (cloud) servers, and software. IoT devices also send and receive data by communicating with apps, databases, or other devices through a network connection. Using these capabilities large number of IoT devices can create high computation power. Attackers use this power to create large-scale botnets.

Arc secure, a device which enables users for secure IoT enabled environment which is targeted on Small Office Home Office (SOHO) use. In Arc secure, Host-Based Intrusion Prevention System (IPS) use for mitigating botnet attacks. This document explains the approach of developing the Host-Based IPS system. The development of the Host-Based IPS is based on selected past researches as well as new research areas which will be explained in the document. The reason for the new approach of the Host-Based IPS is due to the gaps which are present in the current systems for the targeted users.

1.2 Scope

The project involves building a Host-Based IPS for SOHO Networks. Host-Based IPS divided into three subcategories, like IP filtering module, Hybrid Intrusion Detection System (IDS) and Network Monitoring module. The IP filtering module is based on an IP filtering learning module. Hybrid Intrusion Detection System (IDS) contains two sub modules called Hybrid IDS and Host-based IPS which use to identify and mitigate malicious behaviours. Network Monitoring module is monitoring traffic and detect anomalies of the system. These main three modules described in detail in the methodology of this document.

1.3 Overview

The main goal of the project is to deliver a Host -Based IPS for the SOHO network users. The IPS is capable of delivering 24/7 protection to the network from intrusions. The IPS is able to identify protocol-based intrusions as well as anomaly-based intrusions. The task is developing an IDS which is protocol and anomaly based. The anomaly-based IDS is develop using neural-network based intrusion-detection technique. The protocol-based IDS focus its monitoring and analysis on a specific application protocol. Using both methods ARCSECURE able to notify and mitigate anomalies of the system.

2 BACKGROUND AND LITERATURE SURVEY

Recent botnet attacks show high vulnerability of IoT systems and devices. To from basis of this research, literature has been reviewed. In accordance with the [1], explains that common IoT vulnerabilities such as,

- Insecure web/mobile/cloud interface
- Insufficient authentication/ authorization
- Insecure network services
- Lack of transport encryption/integrity verification
- Privacy concerns
- Insufficient security configurability
- Insecure software/firmware
- Poor physical security

In September 2016, an IoT botnet built from the Mirai malware perhaps the largest botnet on record was responsible for a 600 Gbps attack targeting Brian Krebs's security blog (krebsonsecurity.com). Mirai's strategy is quite simple; it uses a list of 62 common default usernames and passwords to gain access primarily to home routers, network enabled cameras, and digital video recorders, which usually have less robust protection than other consumer IoT devices. The same month, a Mirai-based attack against the French webhost OVH broke the record for the largest

recorded distributed denial of service (DDoS) attack at least 1.1 Tbps, and perhaps as large as 1.5 Tbps [2].

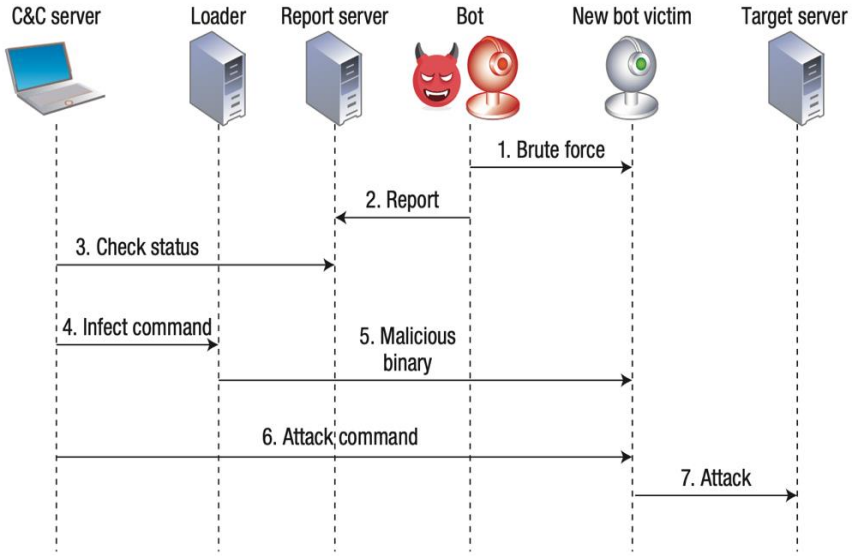

Figure 2.1: Mirai botnet operation and communication.

Figure 2.1 shows Mirai causes a DDoS to a set of target servers by constantly propagating to weakly configured IoT devices. Also, botnet operations and communications done through TCP ports 23 or 2323 and infected devices attempts to spread through port 48101 [2].

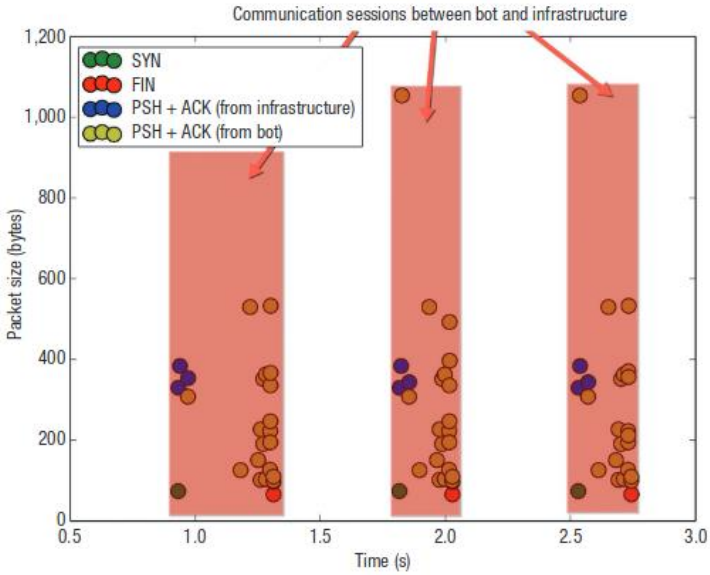

Figure 2.1 Distinctive communication patterns

Figure 2.2 shows communication patterns between an infected IoT device and Mirai's loader component. Analyzing above results, bots leave a footprint that can be identify through basic network analysis. Mirai signatures include [2],

- Sequentially testing specific credentials in specific ports.
- Sending reports that generate distinctive patterns.
- Downloading a specific type of binary code.
- Exchanging keep-alive messages.
- Receiving attack commands that have a specific structure.
- Generating attack traffic with very few random elements.

For detecting attacks launched from IoT bots we propose a Host-based approach, which uses deep learning techniques to perform anomaly-based detection and protocol-based detection. Machine learning comes under protocol-based detection.

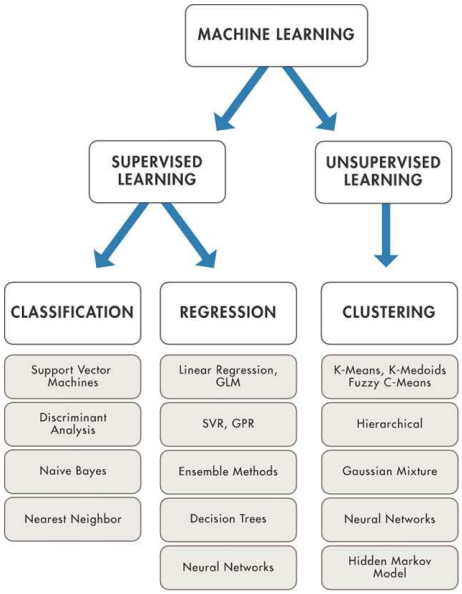

Figure 2.2 Machine learning algorithms

In protocol-based detection, the idea of learning the behaviour of a program has been studied and used actively by many researchers [3]. Gonzalez et al. proposed an intrusion- detection technique based on evolutionary-generated fuzzy rules [4]. The condition part of the fuzzy detection rules was encoded with binary bits and fitness were evaluated using two factors: the accuracy and the coverage of the rule [3].

Propose solution is Hybrid Intrusion Detection System (IDS) with paradigm of learning the behaviour of a program and evolutionary learning together. And anomaly-based IDS use neural-network based intrusion-detection technique.

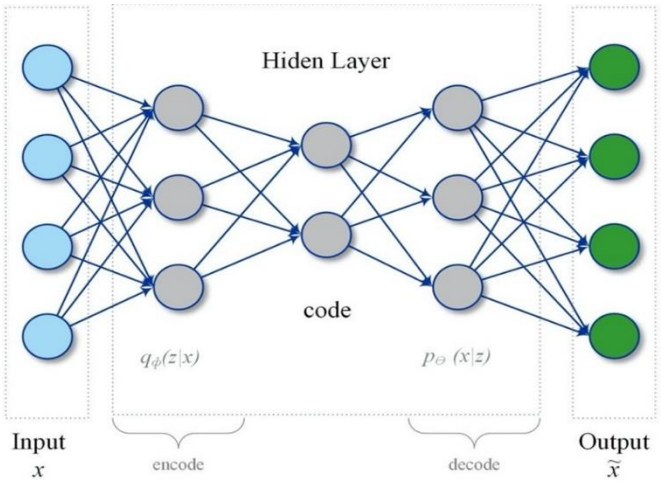

Figure 2.3 Autoencoder Network

Hofmann et al. proposed the evolutionary learning of radial basis-function networks (RBFN) for intrusion detection [5]. They targeted a network-based IDS. Their evolutionary algorithm performed two tasks simultaneously: selecting the optimal feature set and learning the RBFN. The binary-bits system was used to encode the 137 possible features of the network packet headers and three components of the RBFN, including the type of basis function, the number of hidden neurons, and the number of training epochs. In the experiments with the network audit dataset, the RBFN optimized with the evolutionary algorithm outperformed the normal MLP and the normal RBFN [3].

3 RESEARCH GAP

The increasing popularity of the IoT have made IoT environment is powerful amplifying platform for cybercrimes. Recent botnet attacks demonstrate the vulnerability of IoT environment and devices. The Mirai botnet is most recent incident of the industry. Hackers offered Mirai bot nets for rent with as many as 400,000 simultaneously connected devices [2]. Below figure shows different between currently implemented products and what are the weakness of the systems.

	CUJO FIREWALL	F-SECURE	LUMA	BITDEFENDER BOX
ANOMALY DETECTION	N	N	N	Y
TRAFFIC MONITORING	Y	N	Y	N
IDS & IPS	N	N	N	Y
SECURE IP PORTS	N	Y	N	N

Table 3.1 Comparison on features of other devices

The challenge is to implement a mechanism to prevent botnet attacks and efficient, reliable and user-friendly PnP device with minimum resources. Implementing Host-based IPS to keep botnets from taking root in a system. Concentrate additional protections on specific network layer-based vulnerability, such as at point contact between specific IoT device. And also, botnets typically establish communication with one or more remote servers that hackers use to retrieve private information. For that prohibit unwanted traffic from leaving the network and filter data leaving the network.

4 RESEARCH PROBLEM

The problem is to solve how to mitigate botnet attacks? To achieve that, Research needs to fulfil the mentioned research gap with Host-based IPS, That needs to make botnet detection, prevention and monitoring. The ultimate goal is to create a secure connection between the internet and ensure that IoT devices not exploit as zombies.

5 OBJECTIVES

5.1 Main Objectives

Implementing proper mechanism to mitigate botnet attacks and fulfil the mentioned research gap with minimum resources is the main objective of this area. Defenses against conventional botnets can be broadly categorized into prevention, monitoring, and response. Preventing bot infections is the most effective defense. However, machines can become infected despite the use of security techniques. It's therefore critical to monitor network and device behavior for anomalous events or trends that might indicate the presence of a threat. If signs of a potential botnet attack or infected machine are detected, system should prevent and learn the behavior of the attack.

5.2 Specific Objectives

- Disabling open unwanted IP ports of the device.
- Monitoring IP ports 2323/TCP and 23/TCP for attempts to gain unauthorized control over IoT devices using the network terminal (Telnet).
- Monitoring for anomalous traffic on port 48101, as infected devices often attempt to spread malware by using this port to send results to the threat actor.
- Implement way to identify half open connections with learning module.
- Implement IP filtering mechanism.

- Implement protocol-based IDS to monitoring and analysis on a specific device protocol.
- Find suitable machine learning algorithms to detect anomaly of the system.
- Implement anomaly-based IPS to detect any type of misuse that falls out of normal system operation with learning module.
- Implement network monitoring system to monitor incoming and outgoing sensitive data.

6 RESEARCH METHODOLOGY

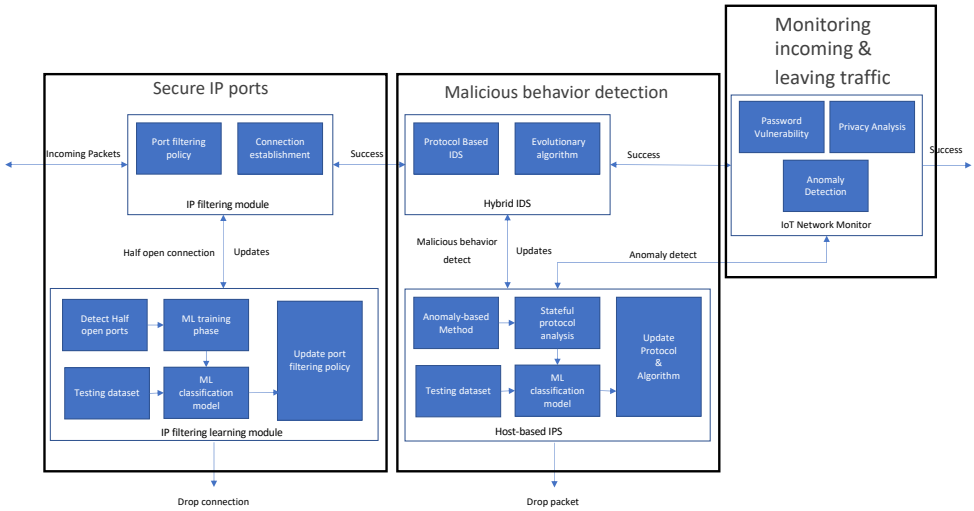

Figure 6.1 Overall system diagram

As illustrated in the high-level diagram incoming packets passes through three modules.

- IP filtering module
- Hybrid IDS and Host based IPS
- Network monitoring module

6.1 IP filtering module

IP filtering module main objective is identifying incoming IP address and establish connection. When identifying process, it checks port address incoming connections trying to reach. Botnet trying to establish connections through TCP ports 23 or 2323.

After that connection establishing process starts. This process contains machine learning phase to verify, its legitimate connection or not. Figure 2.2 shows how to identify distinctive communication patterns. This module also contains port filtering policy its updates when any abnormal behavior detected.

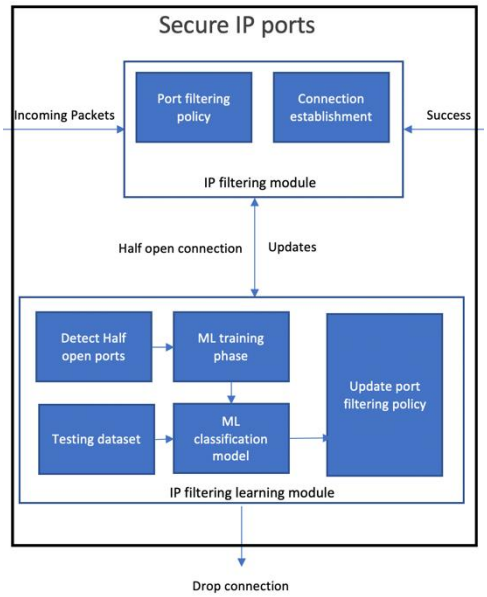

Figure 6.1 IP filtering module

6.2 Hybrid IDS and Host based IPS

In this module system detects malicious behaviors of the packets. This module captures the incoming pcap file and analyze it with the protocol based IDS. Protocol based IDS used to monitor and analyze the protocol (rather than the profile of normal activity it has built) used by that system. The advantage here is that protocols are relatively well-defined (in comparison to "normal activity" profiles), so normal use cases can be created with greater accuracy.

Then it sends to anomaly based IPS, the local audit trail is checked for intrusions. The output is sent to an algorithm to check whether it’s a true positive, data from the local intrusion database is taken for this process. If it’s a false positive the output is discarded and forward the packet if it’s a true positive the local intrusion database is checked for the existence of the respective protocol if the protocol is not present, the local protocol is updated at same time and the packet will be dropped. This use neural network based intrusion detection technique. The main benefit of using a

neural network is the ability to generalize from limited, noisy, and incomplete data. This generalization capability provides the potential to recognize unseen patterns, i.e., not exactly matched patterns that are different from the predefined structures of the previous input patterns [3].

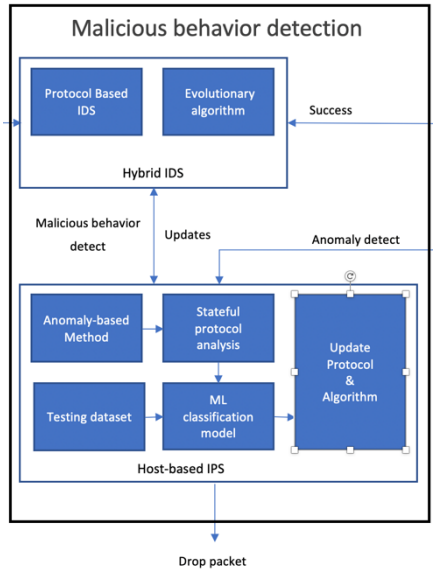

Figure 6.2 Hybrid IDS and Host based IPS

6.3 Network monitoring module

This module include user friendly that integrates with an ARC secure. Network monitor captures packets as PCAP files. Then runs a variety of scripts to parse and analyze the latest PCAP files. It looks for vulnerabilities in three categories [6].

- Password vulnerability
  - Looking for open ports 22 (SSH) and 23 (Telnet) and offering a new password if the password can be cracked using brute force.
- Privacy analysis
  - Check for unencrypted payloads in packet captures containing personal identifiers and other forms of sensitive data (e.g. medical data).

- Anomaly detection
    - Detect IoT botnet DoS traffic originating from an IoT device on the LAN using neural network based anomaly detection technique.

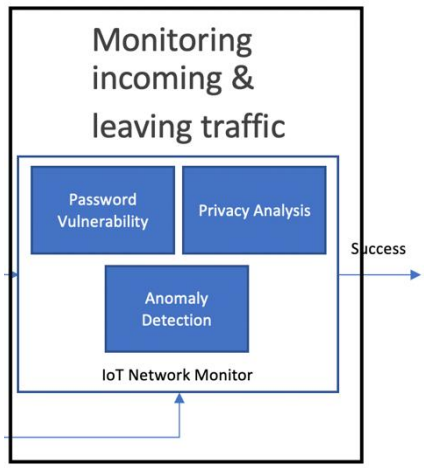

Figure 6.3 Network monitoring module

7 GRANT CHART

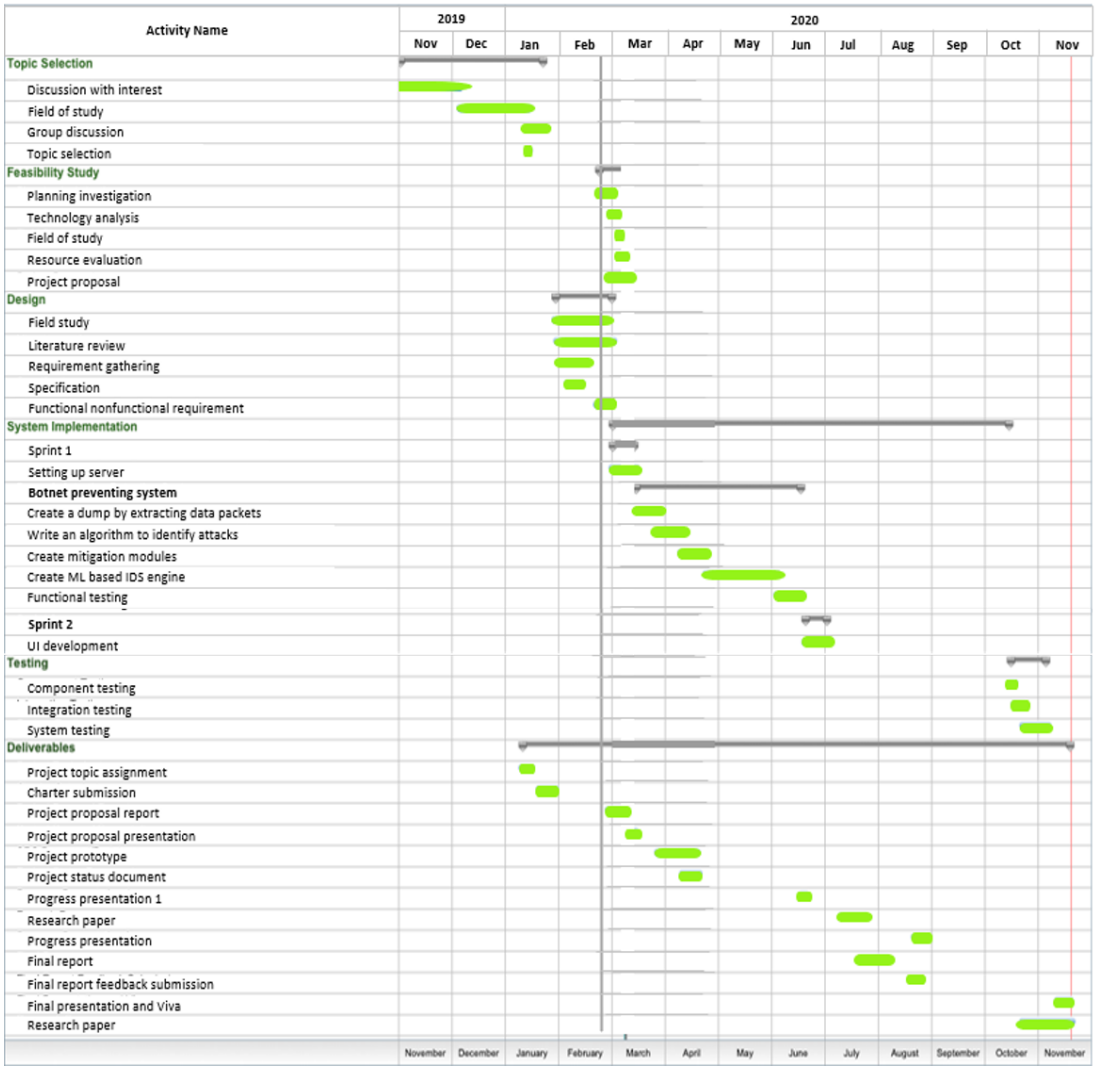

Figure 7.1 Grant Chart

8 PROJECT REQUIREMENTS

8.1 Functional requirements

System should;

- Be able to identify incoming IP address
- Be able to identify open IP ports of the devices
- Monitor TCP port 23 or 2323
- Be able to identify distinctive communication patterns
- Be able to capture incoming and outgoing pcap files
- Be able to analyze pcap files
- Be able to identify anomalies and protocol violations
- Be able to identify password vulnerabilities of the open ports
- Be able to check unencrypted payloads

8.2 Non-Functional requirements

- IoT devices should have local password protection
- IoT devices should be updated
- User portal should be display system traffic

9 BUDGET AND JUSTIFICATION

9.1 Estimated budget for the networking Devices.

Device	Price	Quantity	Total Amount
Raspberry PI	Rs. 16000.00	1	Rs. 16000.00
IoT products	Rs 4000.00	2	Rs. 04000.00
Ethernet Cables	Rs. 500.00	1	Rs. 00500.00
Total Cost			Rs. 20500.00

Table 9.1 Estimated Budget

9.2 Estimated Budget for other expenses.

Items	**Price**	**Total Amount**
Stationary	Rs. 2500.00	Rs. 2500.00
Printing	Rs. 2000.00	Rs. 2000.00
Other	Rs. 2000.00	Rs. 2000.00
Total Cost		Rs. 6500.00

Table 9.2 Estimated Budget for other expenses

9.3 Total Expenses

Description	**Estimated costs**
Estimated budget for the networking Devices	Rs. 20500.00
Estimated Budget for other expenses	Rs. 06500.00
Total estimated cost for the year	Rs. 27000.00

Table 9.3 Total Expenses

10 REFERENCES

[1] E. Bertino and N. Islam, "Botnets and Internet of Things Security," in Computer, vol. 50, no. 2, pp. 76-79, Feb. 2017. [Accessed 22 02 2020].

[2] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, Jeffrey Voas, " DDoS in the IoT: Mirai and Other Botnets," in *Computer*, vol. 50, no. 7, Feb. 2017. [Accessed 22 02 2020].

[3] Xin Yao, "Evolving artificial neural networks," in Proceedings of the IEEE, vol. 87, no. 9, pp. 1423-1447, Sept. 1999. [Accessed 22 02 2020].

[4] F. Gonzalez, J. Gomez, M. Kaniganti, and D. Dasgupta, “An evolutionary approach to generate fuzzy anomaly signatures,” in Proc. 4th Annu. IEEE Information Assurance Workshop, West Point, NY, Jun. 2003, pp. 251–259. [Accessed 22 02 2020].

[5] A. Hofmann and B. Sick, “Evolutionary optimization of radial basis function networks for intrusion detection,” in Proc. Int. Joint Conf. Neural Networks, Portland, OR, Jul. 2003, vol. 1, pp. 415–420. [Accessed 22 02 2020].

[6] G. Jonsdottir, D. Wood and R. Doshi, "IoT network monitor," 2017 IEEE MIT Undergraduate Research Technology Conference (URTC), Cambridge, MA, 2017, pp. 1-5. [Accessed 22 02 2020].