ARCSECURE - CENTRALIZED HUB FOR SECURING A NETWORK OF IOT DEVICES

Project ID: 2020-086

Project Proposal Report

IT17127356 - A.M.S.P.B Atapattu

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

ARCSECURE - CENTRALIZED HUB FOR SECURING A NETWORK OF IOT DEVICES

Project ID: 2020-086

Project Proposal Report

IT17127356 – A.M.S.P.B Atapattu

Supervisor - Mr. Kavinga Yapa Abeywardena

Co supervisor – Ms. Tharika Munasinghe

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 my 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.S.P.B Atapattu	IT 17127356	

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

Signature of the Supervisor: Date:

ABSTRACT

The main purpose of IOT (Internet of Things) is to connect devices with each other which operate over the internet. The biggest challenge in accomplishing this is the risk of security. These devices which are always connected to the internet have access to sensitive information and any security breach is a huge risk.

IOT devices have connected each other and can be operated over the internet making them vulnerable for cyber criminals and other aggressors as well. They can easily have hacked and added to botnets, which are used to launch DDoS against users or organization. To cater to this gap, we propose a plug and play device ‘ARCSECURE’, targeted at small scale and SOHO type business environments. In the solution we propose IoT device will detect and mitigate DoS attacks coming for connected IoT devices with the use of multiple Machine Learning models well trained with both unsupervised and supervised learning techniques. And the propose device will also be enable secure communication over IoT devices using blockchain technology while focusing on affordability and user-friendliness as key factors. In order to avoid DDoS threats secure P2P network will be used to interconnect IoT devices with the support of blockchain technology in a reliable way.

Keywords: Machine Learning, Blockchain technology, Internet Security, IoT DDoS Mitigation

Table of Contents

I List of Figures

II List of Tables

III List of Abbreviations

IOT	Internet of Things
DOS	Denial of Service File System
DDOS	Distributed Denial of Service
SOHO	Small Office Home Office
ML	Machine Learning
HTTP	Hypertext Transfer Protocol

1 INTRODUCTION

1.1 Purpose

The proposed a plug and play device ‘ARCSECURE’, targeted at small scale and SOHO type business environments will provide secure communication over IoT enabled environment with attack detection module for early detection and mitigate any attack, an update automation module as well as a user authorization module all in one, while focusing on affordability. The attack detection is a module which plays major role in this device and DDoS attack detection and enable secure communication over IoT device’s is the subcategory which plays a major role in this module.

Corporate environments buy high end solutions [1] from the providers to secure their IoT devices from cyber attackers. Which is an expensive thing to do to protect the organizations data. 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. We are proposing a comprehensive approach to securely communicate with SOHO IoT devices.

This document explains the approach of developing the DDoS attack detection, mitigation and how to enable secure communication over IoT devices. This research idea of creating an attack detection and enabling a secure connection system is unique and the reason for this unique approach is due to the gaps which present in current attack detection systems in SOHO environments. The technical background, objectives and the Methodology of the research component will be further described in the document.

1.2 Scope

This area of the project involves in building attack detection mechanism and secure communication for IoT enabled environments. This area can be divides into two categories as machine learning based DoS attack detection and secure communication using blockchain technology. This module helps to fully utilize the environment of IoT devices and provide a customer satisfactory communication. Also, this system is connected to a simple plug and play device to get maximum productivity over connected devices.

The main reason to come up with such a project is that, in current IoT enabled environment like SOHO networks [2], there is a lack of affordable and easy to configure technology to properly manage the IoT devices and mitigate potential attacks in the network [3]. When initiating the project, cost and resource management should be done carefully since the project is based on Machine Learning and Blockchain technology, improper development may lead to the need of more resources, thus the targeted audience

1.3 Overview

In current IoT enabled environments there is lack of easy configure technology to properly secure the communication with IoT devices and track down any potential DDoS attacks and mitigate those attacks. Some IoT devices may contain sensitive information that needs to be protected. So, to goal is to use supervised machine learning techniques to detect any data packets that will contain malicious content and it will automatically be dropped in scanning stage in the framework. IoT devices will not get any data packets that will be use the device for DDoS attacks. Here the target audience would-be small-scale enterprises, home based offices or even suitable for home IoT devices.

2 BACKGROUND AND LITERATURE SURVEY

This section depicts a literature survey about the purposed system and its functions. Some of the eminent researches and products are also reviewed here. Since the research is in the domain of networking and internet of things, the final product is designed to plug and play fashion, the development environment has to be configured such that a single codebase can be pushed to multiple peers simultaneously.

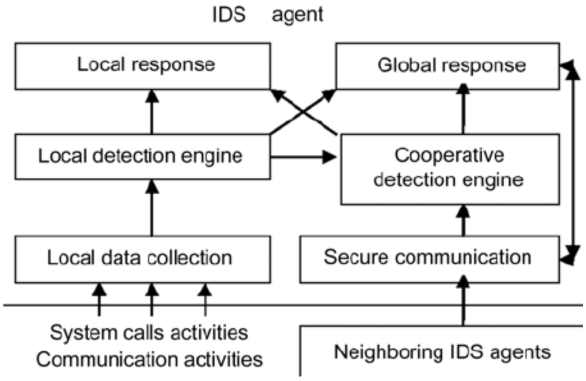
The paper discusses the security risks of SOHO network IoT devices and the vulnerabilities for the course of the risk. The paper categorizes these vulnerabilities into four sections as,

- Service Misconfigurations
- Communication methods
- Insecure by default
- Security and design implementation [6].

From the paper it's clear that vulnerabilities and risks exists in IoT devices and therefore, a mechanism should be practiced to overcome such vulnerabilities [4]. In the paper, it provides some tools to identify vulnerabilities of such networking devices as,

- Nessus
- Nmap
- W3af
- Revok [6]

Shivaramu K and Prasobh P.S discusses in their research paper Security Vulnerabilities that the Wireless Ad-hoc network is vulnerable due to cooperative algorithm, lack of monitoring and management and lack of a particular line of defense [7]. A regular intuition detection system can overcome such problem, the paper proposes a New Architecture to have efficient output [6]. As shown in figure 2.1



1Figure 2.1 IDS model agent

As illustrated in figure 2.1, the first phase it gathers real time data from various sources from a local detection engine and collected data is processed for gathering of evidences for anomalies.

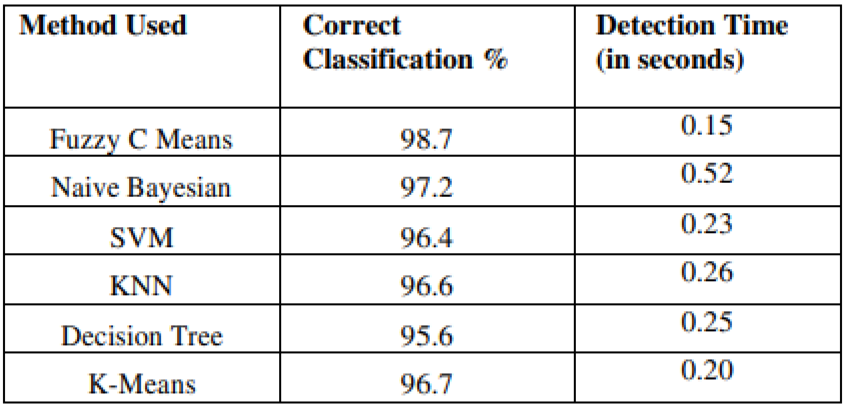
The approach considered is to use feature selection mechanism and build the classifier using various machine learning algorithms such as SVM, K-NN, Fuzzy c-means clustering and decision tree [5]. An important conclusion drawn from the experimental results is that, of the various methods used, Fuzzy c-means clustering is very efficient in detecting DDoS attacks [8].

2.1 Machine Learning Algorithms

In this section all machine learning algorithms that are employed in this proposed framework are briefly described.

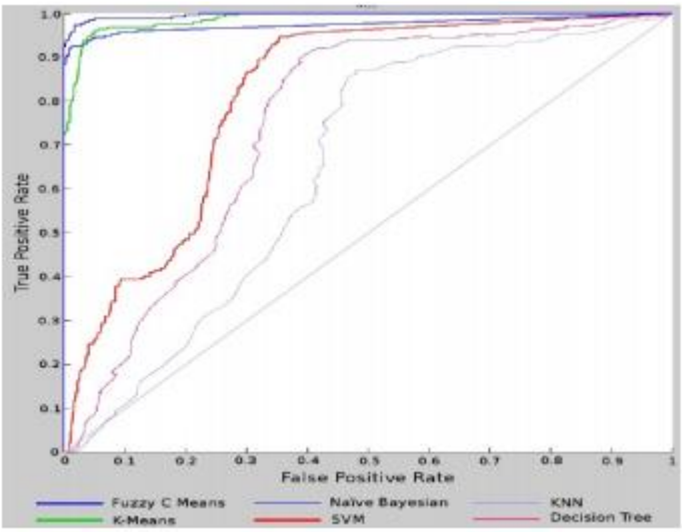
- Native Bayes - The Naïve Bayes is a simple probabilistic classifier [9]. It assumes that the effect of a variable values on given class is independent of the values of other variables.
- C4.5 – This algorithm is based on ID3^2 algorithm that tries to find small decision tree
- K-Mean Clustering - Assignment of the data points to clusters depends upon the distance between cluster centroid and data point.

The research that is done by Suresh M. and Anitha R on Evaluating Machine Learning Algorithms for Detecting DDoS Attacks proves the Fuzzy C Means clustering method gives better classification and it is fast compared to the other algorithms[8] and they used CAIDA dataset [10] for the experiments.



Method Used	Correct Classification %	Detection Time (in seconds)
Fuzzy C Means	98.7	0.15
Naive Bayesian	97.2	0.52
SVM	96.4	0.23
KNN	96.6	0.26
Decision Tree	95.6	0.25
K-Means	96.7	0.20

Table 1 F-Measure details of classifiers [8]



2 Figure 2.3 False vs positive rates [8]

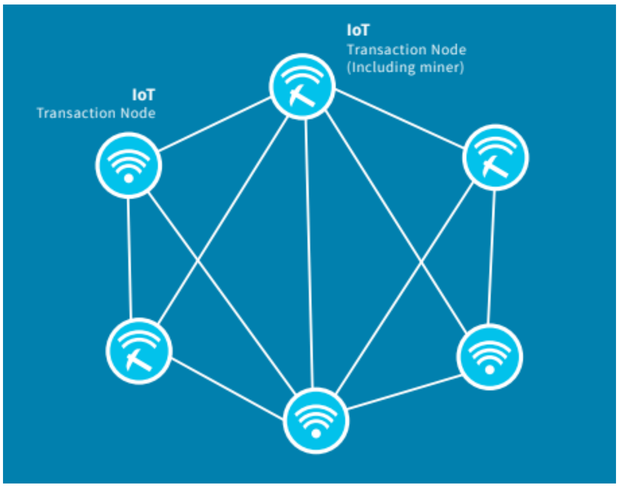
And we are planning to use Fuzzy C Means method for out DDoS detection mechanism on our proposed solution.

2.2 Block-Chain based architecture

Blockchain is a transaction repository where transaction are grouped into blocks. “Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block [11]. The contents of each block are digitally signed to ensure data integrity of recorded transactions.

IoT gadgets can be designed either to create utilize of open blockchain services or to communicate with private blockchain hubs within the cloud over a secure API. Joining blockchain technology into the security system of an IoT framework permits IoT devices to safely find each other, encrypt machine-to-machine exchanges utilizing dispersed key administration procedures, and approve the keenness and authenticity of program picture overhauls, as well as arrangement upgrades

The communication model installation of blockchain software directly on IoT nodes with application programming interface to the IoT nodes. Following figure shows a common and accepted model combining blockchain technology and IoT when the IoT device have capabilities that make them host the transaction node software and maintain the communication across the network of nodes.



3 Figure 2.2.1: IoT node acts as a blockchain transaction node

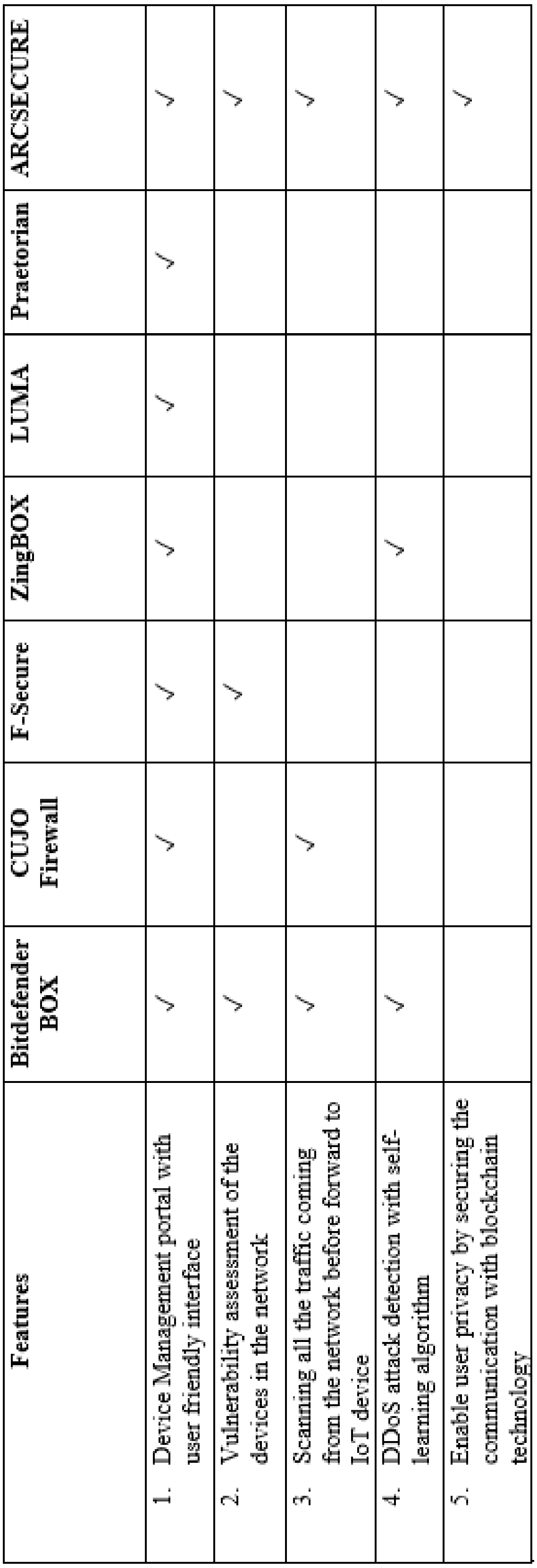
Each device is provisioned with a private key or includes functionality to internally self-generate a private key to participate in network communication. There are some hardware limitations make adopting this model and we plan to provide a solution for this limitation as well.

3 RESEARCH GAP

IoT now has become one of the main business tactics to attract customers, there arise a need of security for these networks because there the users and cybercriminals have the ability to carry out attacks on or via these connections. Usually these issues are resolved by implementing an Intrusion Detection Systems. But when considering a SOHO network, it’s unlikely to find a network with an Intrusion Detection System (IDS) due to their high expenses and complexity. The challenge of this problem is to implement an all in one system which is user friendly and working with minimum resources as current IDS need lot of resources and they are not portable as well.

When secure communication over IoT environment and detect DDoS to the network is considered, there are few attack detection systems which function in static methods. The downsides to these systems are inability to fully utilize secure connection and detect potential DDoS attacks with a single solution, so the challenge of this section is to implement a one single system to address all the following points,

- Analysing all incoming traffic from the network
- Drop any malicious packets arrived from the network and alert user about the recent information
- Protects user’s privacy by enabling secure P2P communication over IoT device and the end user
- Machine learning algorithm is self-learning by scanning all the traffic coming from the network.



Features	Bitdefender BOX	CUJO Firewall	F-Secure	ZingBOX	LUMA	Praetorian	ARCSECURE
1. Device Management portal with user friendly interface	✓	✓	✓	✓	✓	✓	✓
2. Vulnerability assessment of the devices in the network	✓		✓				✓
3. Scanning all the traffic coming from the network before forward to IoT device	✓	✓					✓
4. DDoS attack detection with self-learning algorithm	✓			✓			✓
5. Enable user privacy by securing the communication with blockchain technology							✓

Table 2 Features of ARCSECURE DDoS and Secure communication module

4 RESEARCH PROBLEM

When it comes to small scale businesses and Home offices (SOHO business culture) network security is mostly overlooked.[6] The security of IoT devices should be managed properly.

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 etc. When taking the storage capacity of IoT devices into consideration it will be considerably less, therefore updates aren’t don’t successfully which will in return create loopholes for an attacker to exploit the network of devices.

One of the main security concerns is blocking the attacks for the IoT devices coming from internet by cyber attackers and we purpose to secure it using ARCSECURE. Even though such secure mechanisms are available, they are both unaffordable and not user friendly for a small scale and SOHO type business due to their budgets and not having trained cyber security or IT personnel. The purposed solution is a combination of supervised and unsupervised machine learning methodologies and blockchain technologies to identify certain attack types with the help of pre-loaded data sets continuously self-learning machine and secure the communication mechanisms with the IoT device and the user, it will be able to capture and analyze any malicious packets that are coming from the network. Maintenance will also be easy as well as it will be more efficient in detecting malicious data packets as it will learn along the way.

5 OBJECTIVES

5.1 Main Objectives

The main objective of the research is to provide a plug and play device targeting for IoT enabled environment of SOHO business environments and small-scale businesses to provide a secure communication and risk-free experience with a well-secured IoT environment. Most of the networking IoT devices are very difficult to maintain because of the lack of security issues and lack of knowledge on these devices. There should be a proper mechanism to protect IoT devices to take the maximum use of that device as well as to get maximum security out of that device. Most of the time organizations have to pay a huge amount of money to hire an expert to configure these devices and it takes more time to get the final usability of that device. The proposed device 'ARCSECURE' will be able to adopt to the network and do the needed configurations by itself. Even without a thorough knowledge in IT, the users will be able to get the similar productivity provided by proposed device achieved with unsupervised and supervised machine learning techniques and blockchain technology.

5.2 Specific Objectives

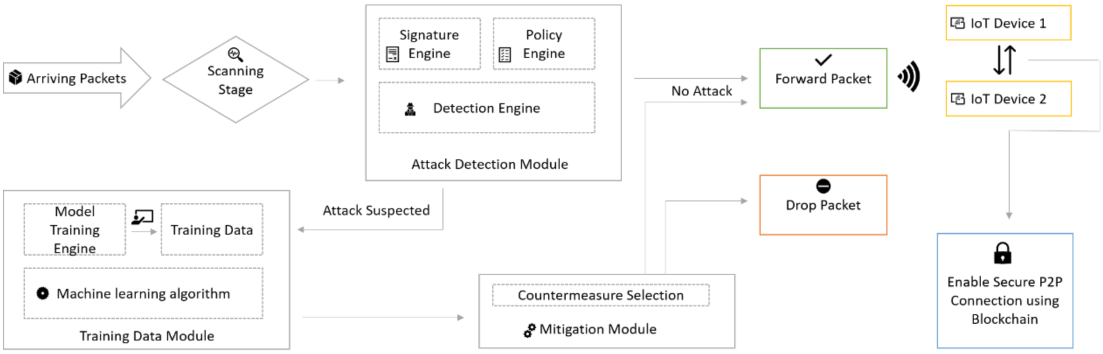
- Create a way to implement backend of the IDS to collect all the packets passing through.
- Implement the IDS engine to process the collected packets to capture any intrusion attempt of any data packet.
- Identify a method to notify the user when an any malicious data packet is found and store the collected details in a Db and use that information to train the ML algorithm.
- Identify a Machine Learning algorithm for find malicious data packets when scanning process.
- Identify a method to secure the communication between IoT devices.
- Implement a process to identify and analyze the malicious packets receiving trough the network daily basis.

- Identify number of users connected and using IoT devices over the network and alert them for any intrusion attempts using a method of communication
- Identify a tactical way to learn Machine Learning algorithm by itself using receiving data packets and pre-defined configurations.
- Implement policies to track all incoming packets other than using only Machine Learning algorithms.
- Create signature-based engine for attack detection module for support the scanning stage of the module
- Implement mechanisms for countermeasure selection to mitigation module for received data packets after the ML training process.

6 RESEARCH METHODOLOGY

This section will explore the research components and the methodology in which the research workload is carried out to build the plug and play device **ARCSECURE**. The final output of this research is a portable device with 4 core functions. One of those core functions is enabling secure communication over IoT devices while detecting DDoS threats to utilize and communicate IoT devices with a proper manner. Eg: By analyzing all data packets coming from the internet to the device and learn ML algorithm using that information. The whole process is illustrated in Figure 8.1.

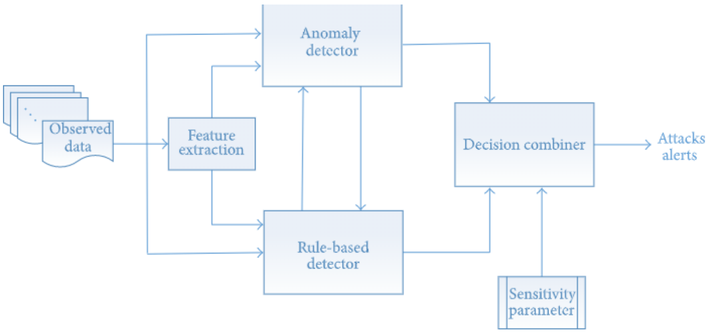
In this function we will be managing all the incoming data packets in advanced scanning process considering few pre-defined variables and our ML algorithm. There are three main modules in this function and those functions methodologies are described in following. We are introducing this method to utilize and communicate IoT devices and give customers an outstanding risk-free secured experience.



4 Figure 8.1: DDoS attack detection and enabling Secure connection

6.1 Attack detection Module

All incoming traffic will be going through this module for complete the scanning process of this function and this module contain Signature and Policy engine. DDoS attacks can be detected by examining of the network traffic changes. In study performed by Chonka et al. [4], by using the property of network self-similarity a model is developed to find out DDoS flooding attack traffic. The parameters of the detectors are controlled by a centralized node. The design goal of this intrusion detection system is to enhance the overall performance of DDoS attack detection, by shortening the detection delay, while increasing the detection accuracy and seed of the network communication. The block diagram is show in figure 8.1.1. As in the figure the data containing normal traffic and DDoS attacks is processed some features and then the data linked to signature-based detector blocks to detect attacks.



5 Figure 8.1.1: Proposed model of IDS for signature-based attack detection

6.2 Data Training Module

In this module we a purposed to train the machine using data which have been gathered for training purpose and the second approach is to test the captured data. Well trained ML algorithm will clearly classify the abnormal patterns from normal data packets. It will easily identify any anomalies inside the IoT environment.

ML training datasets are commonly available and have lots of redundant information which will make the attack discovery process and classification method inefficient such as KDDCup’99[5] and this dataset have various well-known attack variants, but since attacks are constantly upgrading these old datasets do not have samples for new DDoS attack methods such as Hypertext Transfer Protocol flood and Structured Query Language Injection Distributed Denial of Service attacks and we plan execute various attacks instances in a controlled IoT network environment.

6.3 Mitigation Module

This will be the final module in the framework and all incoming network traffic will also be going through here for IoT devices or if the purposed system will be able to detect any anomalies the packets are dropped in this stage as well.

6.4 Gantt Chart

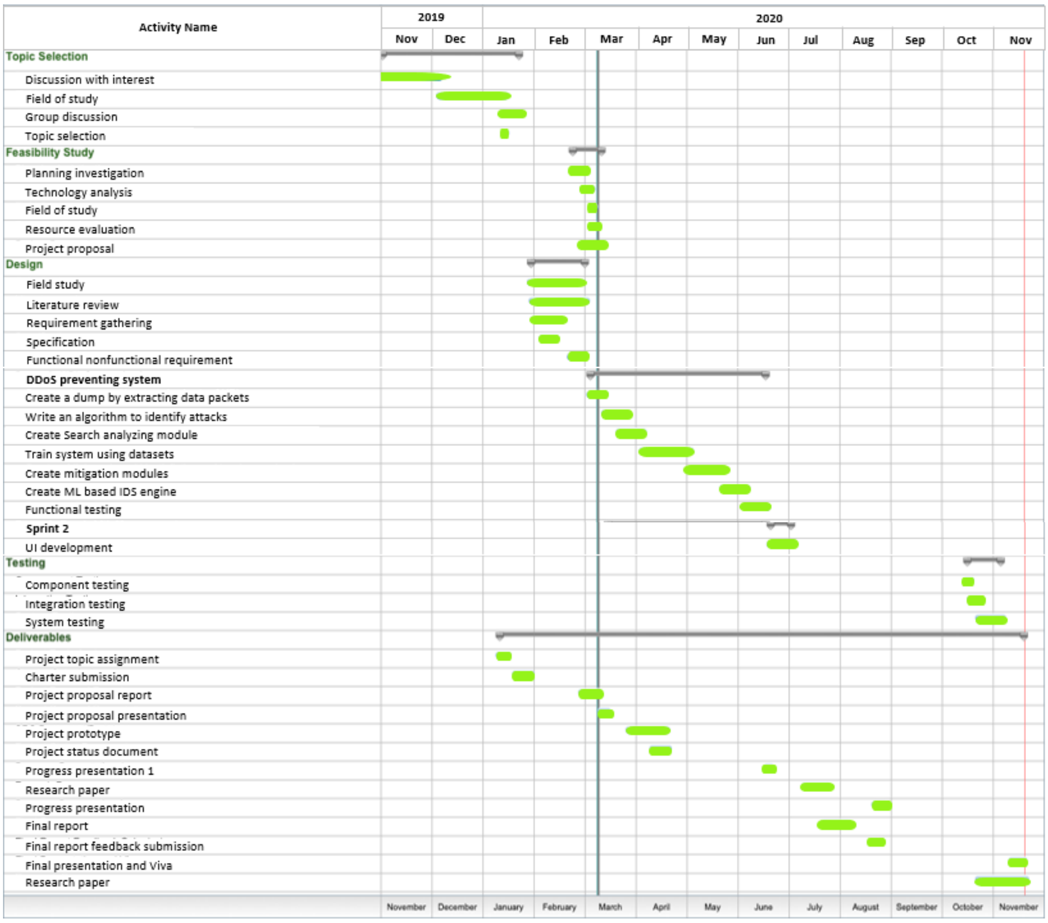


Table 3 7 Gantt Chart

7 DESCRIPTION OF PERSONAL AND FACILITES

The workload of this research is assigned to a group of four members where each member has an equal workload to complete

7.1 DDoS attack detection and enable secure communication. A.M.S.P.B Atapattu – IT17127356

- Requirements Gathering
- Extraction of packet data which passes through the network create a dump.
- Creation of a Machine Learning Based Intrusion Detection Engine.
- Creation of local Database to store the Intrusions that are identified.
- Develop an Intrusion detection alarming system.
- Using Blockchain technology to enable secure communication between IoT devices

8 PROJECT REQUIREMENTS

8.1 Functional Requirements

- Scan all the packets that are going through the network.
- Find any anomalies in the network.
- Mitigate any DDoS attacks.
- Identify any DDoS threats and alert user.
- Enable secure communication between devices.
- Identify malicious behavior.

8.2 Non-Functional Requirements

- Performance
- Security
- Availability
- Reliability
- Maintainability
- Usability

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 4 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 5 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 6 Total Expenses

10 REFERENCES

[1] A.J Gold, " jgoldassociates.com," Bussiness Environment: is it Safe, 2016. [Online]. Available: http://jgoldassociates.com/White_Papers/Android_in_the_Business_Environment_Whitepaper.pdf . [Accessed 18 Feb 2020].

[2] Stylianos Kavalaris and Emmanouil Serrelis," Multimedia Implementations for SOHO Networks and Their Security Issues " International Journal of Cyber-Security and Digital Forensics , AMC Metropolitan College , 2015.

[3] Nikolai Hampton and Patryk Szewczyk, " A survey and method for analysing SoHo router firmware," , 2015. [Online]. Available: https://ro.ecu.edu.au/ism/176/ [Accessed 20 Feb 2020].

[4] A. Chonka, J. Singh, and W. Zhou, “Chaos theory based detection against network mimicking DDoS attacks,” IEEE Communications Letters, vol. 13, no. 9, pp. 717–719, 2009.

[5] KDDCUP99, “Machine learning Data files” (2019). [Online] Available: https://datahub.io/machine-learning/kddcup99 [Accessed 19 Feb 2020]

[6] Hatalová, M. (2015). Security of small office home routers.

[7] [Zhang, Y. and Lee, W. Shivaramu K.Na, Prasobh P.Sa , Nagaraj Potia (2016). [online] pdf.sciencedirectassets.com. Available at: https://pdf.sciencedirectassets.com/282073/1-s2.0-S2212017316X00059/1-s2.0-S2212017316304832 [Accessed 20 Feb. 2020].

[8] Suresh, M., & Anitha, R. (2011). Evaluating Machine Learning Algorithms for Detecting DDoS Attacks. [online] link.springer.com/ Available at: https://link.springer.com/chapter/10.1007/978-3-642-22540-6_42

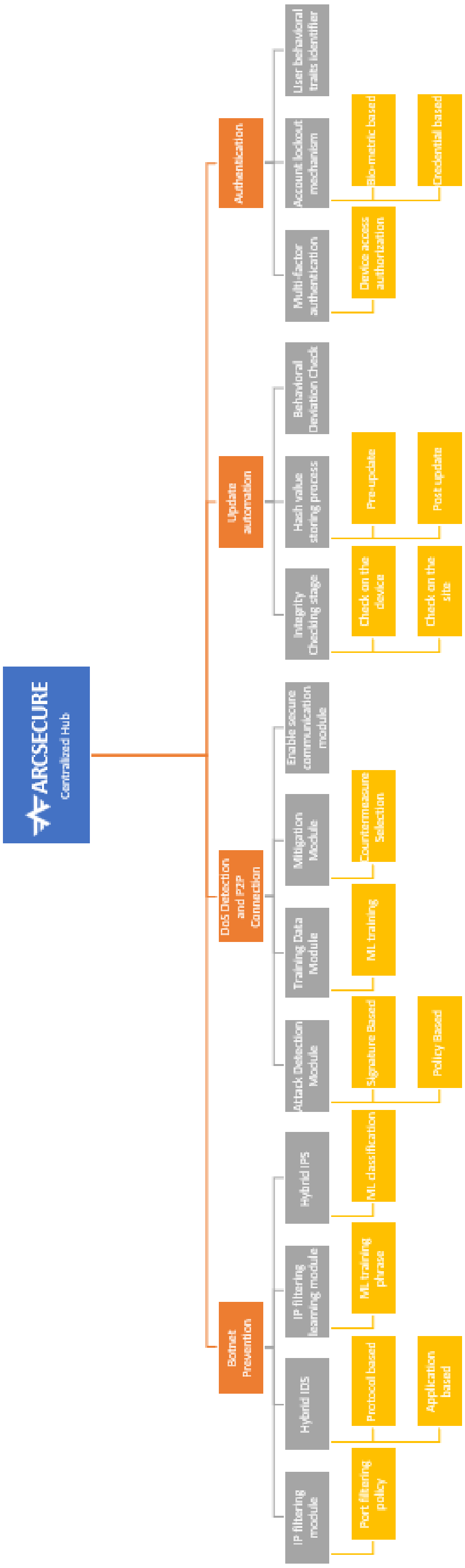
[9] Mitchell, T.: Machine Learning. McGraw Hill, New York (1997)

[10] . UCSD Network Telescope – Code-Red Worms Dataset. The Cooperative Association for Internet Data Analysis (2001)

[11] Block chain, [Online] Available: https://en.bitcoin.it/wiki/Block_chain [Accessed 21 Feb 2020]

11 APPENDICES

11.1 Work Breakdown Structure


ARCSECURE
Centralized Hub
Authentication
Update automation
DoS Detection and P2P Connection
Botnet Prevention
User behavioral traits identifier
Account lockout mechanism
Multi-factor authentication
Bio-metric based
Credential based
Device access authorization
Behavioral Deviation Check
Hash value storing process
Integrity Checking stage
Pre-update
Post update
Check on the device
Check on the site
Enable secure communication module
Mitigation Module
Training Data Module
Attack Detection Module
Countermeasure Selection
ML training
Signature Based
Policy Based
Hybrid IPS
IP filtering learning module
Hybrid IDS
IP filtering module
ML classification
ML training phrase
Protocol based
Application based
Port filtering policy