ARCSECURE - CENTRALIZED HUB FOR SECURING A NETWORK OF IOT DEVICES

Project ID: 2020-086

Project Statues Document I

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

July 2020

ARCSECURE - CENTRALIZED HUB FOR SECURING A NETWORK OF IOT DEVICES

Project ID: 2020-086

Project Statues Document I

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

July 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:

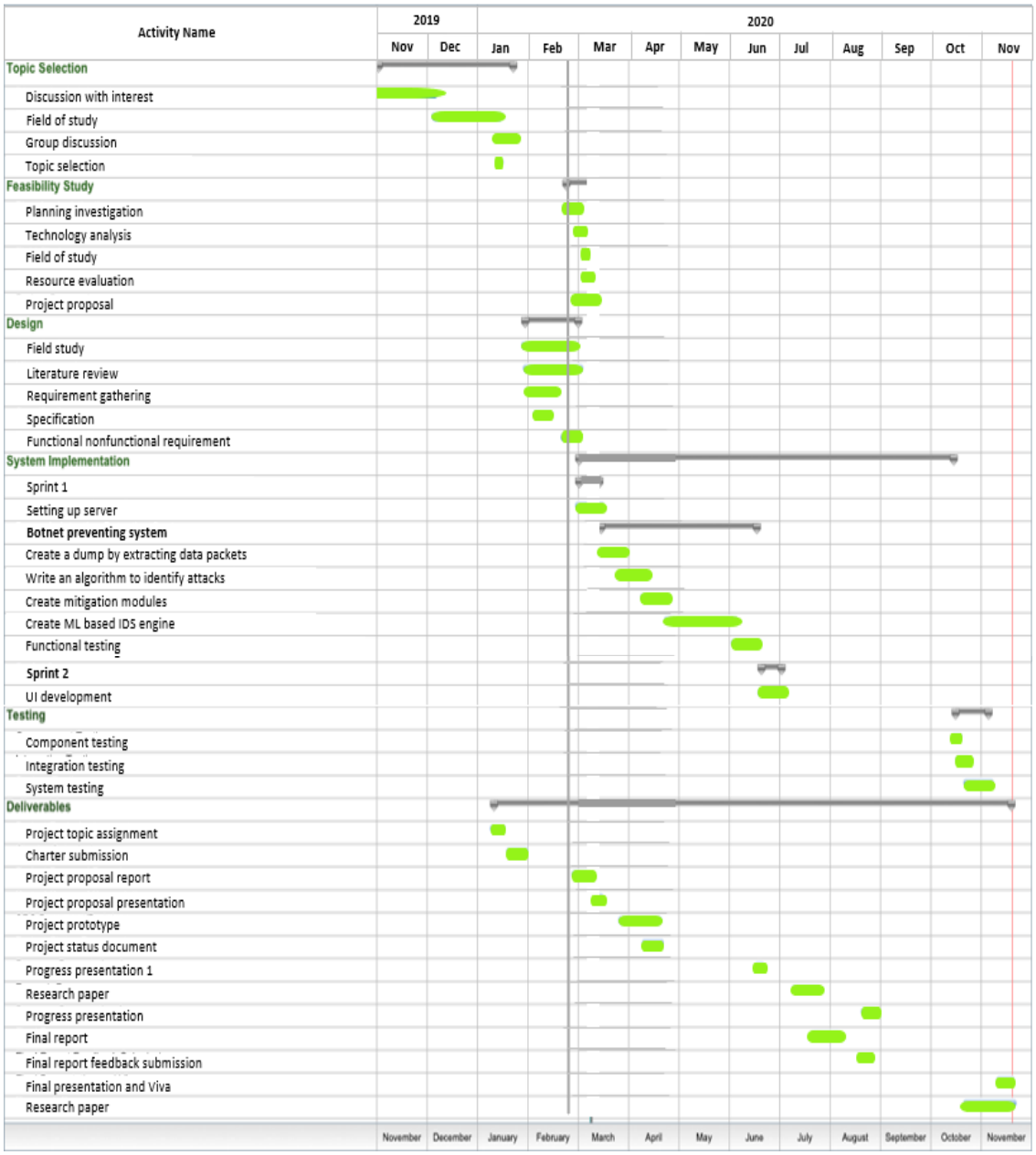
Table of Contents

Introduction

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.

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.
Project Timeline.

Updated Gantt Chart



Work Breakdown Structure (Achieve deadlines)

Task	Estimated		Actual	
	Strat	End	Start	End
Server Configuration	05/01/2020	25/04/2020	25/02/2020	15/05/2020
Network Structures Analysis	10/02/2020	20/02/2020	01/03/2020	25/03/2020
Data set Analyzing	05/03/2020	25/03/2020	25/03/2020	15/04/2020
Model Development	10/04/2020	20/04/2020	01/05/2020	25/06/2020
Find required ML Algorithm	05/04/2020	25/04/2020	25/04/2020	15/05/2020
Analyze performance	10/06/2020	20/06/2020	01/07/2020	10/07/2020
Training with Data set	05/05/2020	25/05/2020	25/06/2020	05/07/2020

Finalize work breakdown structure

Task	Estimated		Actual	
	Strat	End	Start	End
Network UI Implementation	05/07/2020	25/08/2020	10/07/2020	-
Frontend Development	10/09/2020	20/09/2020	-	-
Testing	25/09/2020	30/09/2020	-	-

Project Management Tool

Milestones

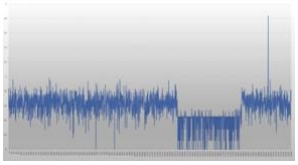
- Network structure analyzing
- Dataset Analyzing
- Model Development
- Finding required Machine learning algorithm
- Analyzing Algorithm performance
- Training with dataset

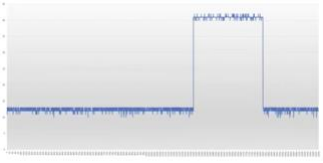
Test Results

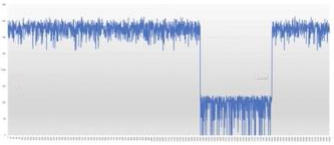
The whole point being to end up with a usable hardware implementation, it is impossible to afford more than a few milliseconds for each packets on a rather weak machine And take the time to benchmark the performance of other well-known algorithms.

SVM Training Parameters

- Speed of source IP
- Standard deviation of flow packets
- Standard deviation of flow bytes
- Speed of flow entries
- Ratio of pair-flow entries

SSIP 

SDFP 

SDFB 

User Task Allocation details

Task	Estimated	
	Strat	End
DoS Detection module	05/04/2020	10/07/2020
Mitigation Module	10/05/2020	20/08/2020
Network UI	25/06/2020	30/09/2020

Documentation Work

1. Project charter-Completed
2. Project proposal-Completed
3. Project status document-Completed
4. Progress Presentation I -Completed
5. Research Paper-Pending

Supervisor Meeting Screen Shots