IoT Mini Project

Using Deep Learning to Increase IoT Security

Ram T N	(108118078)
Sai Mitheran	(108118084)
S Srivaradharajan	(108118100)
V Sai Vignesh	(108118108)

Topic - Detection of IoT BotNet Attacks

Table of Contents -

Project Team Details

Name - Ram T N
Roll Number - 108118078
Class - ECE B
Phone - 9884052296
Email - ram20.91999@gmail.com

Name - Sai Mitheran
Roll Number - 108118084
Class - ECE B
Phone - 9600523852
Email - saimitheran06@gmail.com

Name - Srivaradharajan S
Roll Number - 108118100
Class - ECE B
Phone - 9790994732
Email - srivaradharajan.0112@gmail.com

Name - V Sai Vignesh
Roll Number - 108118108
Class - ECE B
Phone - 9694206942
Email - v.saivignesh2000@gmail.com

About the Mini Project

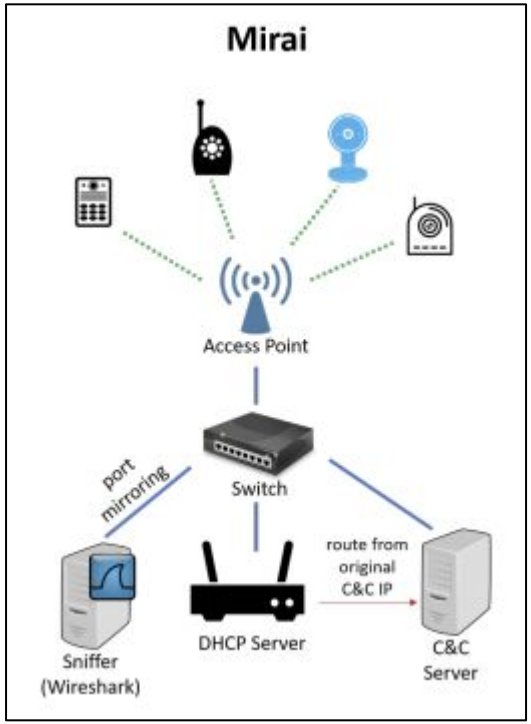
Detection of IoT Botnet Attacks

Internet of Things is a network in which all physical objects are connected to the network devices or routers and can exchange data. In general, it is an ecosystem consisting of web-enabled smart devices that use embedded systems, such as **processors, sensors and communication hardware**, to collect, send and act on data that they acquire from their environments. It is an integral part of our everyday life and its usage exponentially increased over the years. Managing these connected devices has become challenging, particularly due to **cyber-attacks**. It is now very easy to hack a centralized controller connected to an IoT network to get the access of the complete system.

Our goal is to use **Deep Learning** on publicly available botnet datasets to train the model, and further test the model in real-time using a simulated Botnet attack to an IoT Network. The datasets contains real traffic data gathered from 9 commercial IoT devices authentically infected by **Mirai** and **BASHLITE**. Primarily, our aim is to distinguish between **Benign** and **Malicious** traffic data by means of anomaly detection techniques. Since the malicious data can be divided into 10 attacks carried by 2 botnets, the collected data can also be used for **multi-class classification**: 10 classes of attacks, plus 1 class of 'benign'.

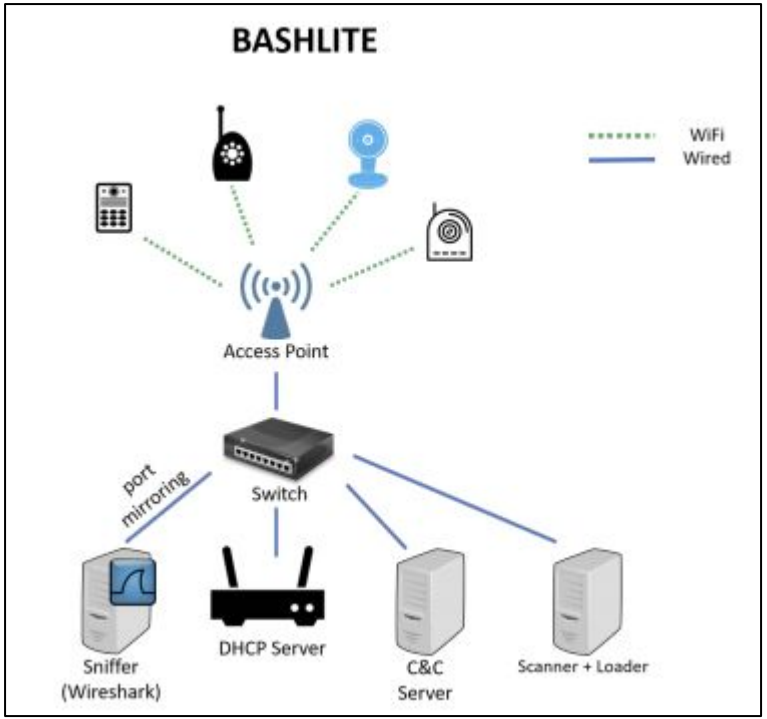
Deep Learning architectures have gained more attention in recent years compared to other traditional machine learning approaches in different fields of AI. One advantage of Deep Learning techniques is that it can learn **hidden features** from the raw data. Each layer trains on a set of features based on the **previous layers' outputs**. IoT devices can be identified with high accuracy based on their network behaviour and sets a stage for future work in detecting specific network activity causing **security breaches** in **smart IoT environment**. Our project has the ability to provide a different outlook and approach to device classification that can eventually help improve the future of IoT and its success in this globalizing world.

General Botnet Attack Environment



At its core, Mirai is a self-propagating worm, i.e., it's a malicious program that replicates itself by finding, attacking and infecting vulnerable IoT devices. It is also considered a botnet because the infected devices are controlled via a central set of command and control (C&C) servers. These servers tell the infected devices which sites to attack next.

It is a renowned Internet-of-Things botnet that took down major websites via massive distributed denial-of-service using hundreds of thousands of compromised Internet-Of-Things devices. These attacks were carried out via small IoT devices like home routers, air-quality monitors, and personal surveillance cameras. Mirai was so viral that it infected over 600,000 vulnerable IoT devices.



Bashlite was used in large-scale **DDoS attacks** in 2014, but it has since crossed over to infecting IoT devices. In its previous iterations, Bashlite exploited **Shellshock** to gain a foothold into the vulnerable devices. An attacker can then remotely issue commands particularly, to launch DDoS attacks, and download other files to the compromised devices.

Abstract

A steady increase in usage of IoT devices which are more vulnerable to security compromises than desktop computers has led to an increase in the occurrence of IoT-based botnet attacks. To mitigate this new threat, a deep learning model is presented in this project. This deep learning model uses a publicly available dataset for pre-training, which will be further fine-tuned on scraped data and smaller datasets. Furthermore, we'll make an IoT network, and try to attack the network with malware and show the effectiveness of the model.

Bill of Materials (Hardware and Software)

Software -

1. **Python** programming language

2. Python Libraries - **Pandas, Numpy**, **Scikit-Learn** etc.

3. **Keras** with **Tensorflow Backend**, **Pytorch**

4. **Selenium/Scrapy** for Web Scraping, **Beautiful Soup** for Parsing

5. **API for Botnet Attack Simulation (In Development Phase)**

Hardware -

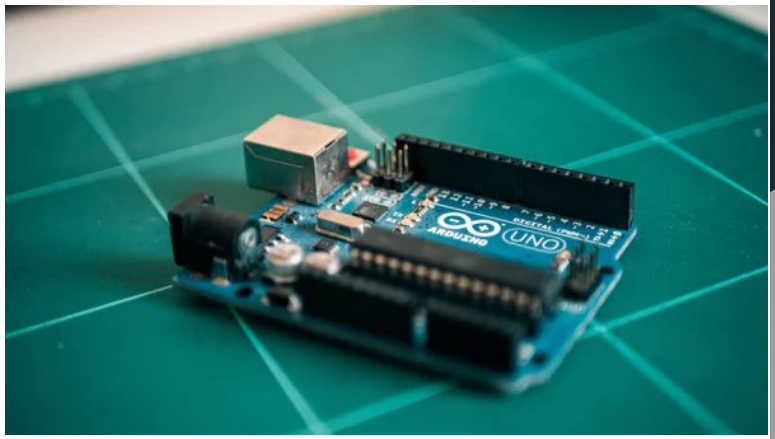
Our models are trained on one machine with a single **Tesla P100-PCIE-16GB** or a **Tesla T4 GPU** at **1.59GHz**. The machine used is a **VM with 12.72 GB RAM,** using an **Intel Xeon CPU at 2.2 GHz.** These are made available by **Google Colaboratory** and **Kaggle's Kernel**, providing free Cloud Computing Services. Further, the use of Arduino and a WiFi module is being looked into, and might be required to simulate a malware attack.

In case the RAM available through **free** cloud compute services are not sufficient, we plan to rent a **CPU-Optimized Droplet** from **Digital Ocean**. They provide **Compute-optimized virtual machines** with dedicated hyper-threads from best-in-class Intel CPUs for workloads at subsidized rates.

Tesla P100-PCIE-16GB GPU

Intel Xeon CPU at 2.2 GHz

Arduino UNO Board



Tesla T4 GPU

Digital Ocean - Rental

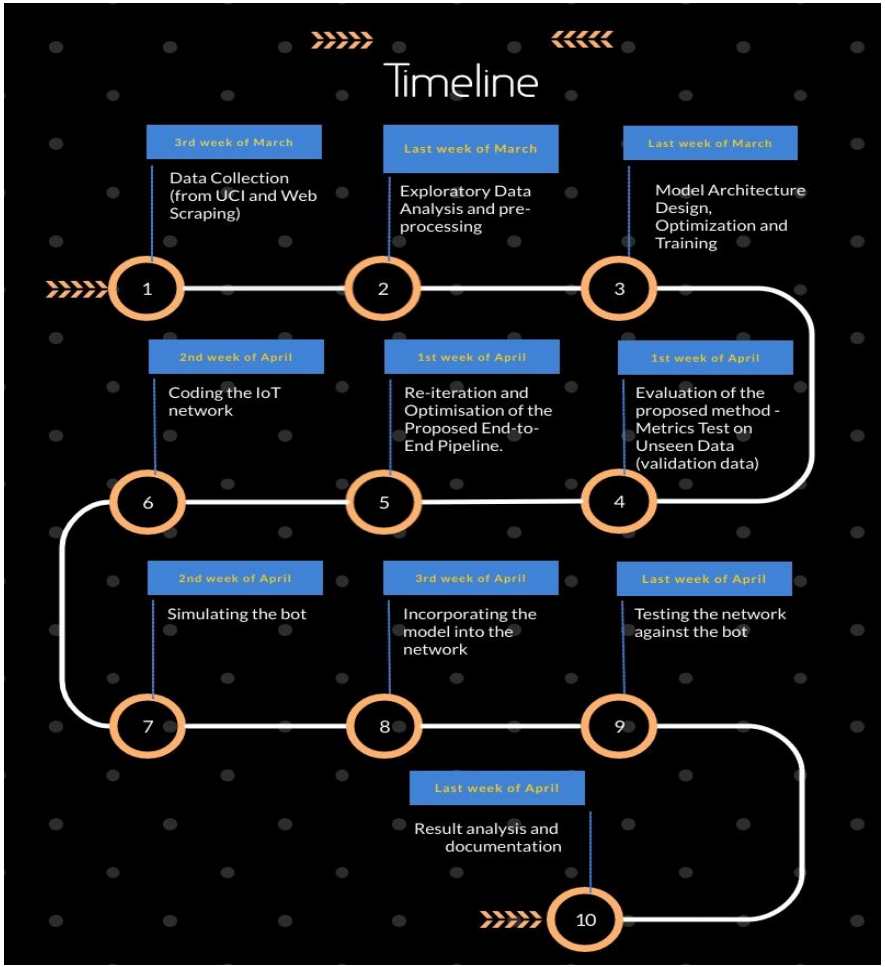
CPU-Optimized

The CPU-centric Droplet, with 100% dedicated vCPU, along with a more modest 2GB of memory for each vCPU.

DESIGNED FOR

CPU-intensive applications like CI/CD, video encoding, machine learning, ad serving, batch processing, and active front-end web servers.

Flowchart of the Project Implementation



Thank you for your time