Project ID:18	**Title: Anomaly Detection and Classification of IoT Attacks using Autoencoders and Multi-Output DNN** **Domain: Networks, IoT and DL**

Abstract: Botnet attacks are responsible for the largest Distributed Denial-of-Service (DDoS) attacks on record. The detection of botnet attacks has become crucial now more than ever due to the frequent emergence of newer botnets and botnet attacks . An increase in vulnerable connected devices, and continued growth in the DDOS-as-a-service industry ensures relevance of botnets as a threat.

IoT devices focus on maximizing functionality whilst reducing resource utilization. Due to this, it becomes incredibly difficult for IoT device manufacturers and programmers to include complex cryptographic mechanisms and security measures in the framework of these devices. These reasons make IoT devices an easy target for attacks.

Thus, the purpose of the project is to detect unknown attack data from known data and further classify the known data into respective botnet and attack types which is done in two phases. To perform the unknown attack detection, a dataset has been generated by simulating an unknown botnet attack in a virtualized environment. The first phase involves anomaly detection of unknown attacks using Autoencoders. The second phase consists of multi-output classification of the detected known data using Multi-Output DNN into botnet and attack types. Hence, one of the benefits of the approach is that it overcomes the problem of detecting unknown or newer botnet attacks that may emerge. Moreover, this approach performs multi-output classification which is a technique that existing papers have not explored. Thus, this project provides a holistic approach to detect IoT attacks including unknown attacks.

Team:

Maria Abraham Pynadath
PES2UG19CS224

K J Pavithra
PES2UG19CS278

Sahil Elton Lobo
PES2UG19CS348

Sanjana S Murthy
PES2UG19CS364

Supervisor: **Dr. Bharathi R**

Architecture diagram