**Botnet Detection and Intrusion Prevention using Deep Learning**

Nilay Anand, Trieu Vo

College of Professional Studies

Logo

Description automatically generated

EAI 6980: Integrated Experiential Capstone

Professor Mimoza Dimodugno

**Project Description**

Botnets are a growing concern in today's digital landscape, as they pose a serious threat to computer systems and networks. A botnet is a network of compromised devices that are controlled by a single entity, typically for malicious purposes. These devices can include computers, smartphones, routers, and other internet-connected devices.

The goal of this project is to train a learning model using a large dataset of network traffic to distinguish normal traffic from botnet traffic. The application of such a system will be highly beneficial for organizations and save time, money, and resources.

The methodology consists of using the CTU-13 dataset containing data packets captured over a monitored network. It has data from 13 different capture sessions with a unique botnet in each session from a set of 6 botnets. The problem is complex due to the data being highly skewed with less than 10% of the data consisting of botnet traffic. The algorithms tested are traditional machine learning algorithms (Random Forest, XGBoost and Light GBM) and neural networks. The results using Machine learning models have been better than Deep Learning with the tree-based algorithms achieving more 99% accuracy and the artificial neural network stuck at 86% accuracy on the test data. The results of tree-based models are equally impressive on unknown test data with more than 99% prediction rate for the same type of bot. The model selection is done based on false negativity rate. The final model achieved a similar accuracy of more than 99% with an unknown botnet not used as part of training.