Cyber Smart Security: Artificial Intelligence for Network Intrusion Detection Systems

Fouse, Lian (School: President William McKinley High School)

This project compares eight artificial intelligence models for detecting cyber attacks. The purpose of this project is to address the rising frequency and severity of cyber attacks that are exposing sensitive personal information and costing billions of dollars. One layer of defense against cyber attacks is a Network Intrusion Detection System (NIDS), which analyzes incoming network traffic and blocks packets that are identified as malicious. Current NIDS tend to be signature-based, which struggle at detecting new types of attacks, or anomaly-based, which have high false alarm rates. Artificial intelligence models investigated in this project hold the potential to identify zero-day attacks while maintaining a low false alarm rate. The specific models compared in this project were Support Vector Machines, K-Nearest Neighbors, Decision Trees, Random Forests, Gradient Boosted Trees, Multilayer Perceptron Networks, Convolutional Neural Networks, and Recurrent Neural Networks. The dataset used to train, tune, and evaluate the models contains over 2.8 million instances of network traffic including both benign activity and common cyber attacks. The models were tested on a binary classification task (benign vs malicious traffic) and a multiclass identification task (individual attacks need to be distinguished). Random Forests, an ensemble method that combines outputs from multiple decision trees, outperformed all other models in both tasks, correctly identifying 99.72% of network traffic in the binary task. This outcome demonstrates the viability of using artificial intelligence to detect cyber attacks with great accuracy. The development of AI-enhanced NIDS shows great promise for reducing the frequency of destructive security breaches.