ABSTRACT

At this time, the development of Internet of Things (IoT) application networks is growing very rapidly. This growth leads many hackers to carry out more active attacks on IoT networks. e.g. DDoS, DoS, Mirai, recon, etc attacks that can attack the confidentiality, integrity, and availability of the IoT network. therefore a security system technology is needed to be implemented on the IoT networks.

Intrusion Detection System (IDS) is an example of technology that can prevent these attacks. In order to detect anomalies and invisible attacks accurately, machine learning classifiers lead to more robust performance in IDS. There is a lot of normal data in network traffic, but abnormal data only accounts for a small part of the network traffic. However, some single machine learning classifier algorithms with class imbalance problems generally have low performance and accuracy in detecting detailed attack types.

Considering the class imbalance in large-scale network flow data, this research presents a double layer network intrusion detection model based on machine learning using a boosting algorithm for IoT environments. The CICIoT2023 dataset is used in this study for training and testing the machine learning model as a simulation of real network data in IoT networks. The proposed approach consists of two layers that work sequentially, where the first layer is to detect normal and abnormal classes with categorical boosting (CAB) algorithm and the second layer is to detect detailed classes such as BruteForce, DDoS, DoS, Mirai, Recon, Spoofing, Web, or Benign with extreme gradient boosting (XGB) algorithm. The results show that the boosting algorithm used has potential in real-time IoT networks.

Keywords: IoT, IDS, machine learning, double layer, categorical boosting, extreme gradient boosting.