Abstract

Internet of Things (IoT) is a network between computing devices that has the ability to send data over a network without requiring human interaction. IoT has the benefit of making human work easier, but on the other hand IoT also has a weakness, namely being vulnerable to cyber attacks. Denial of Service (DoS) is one of the attacks that often occurs in the IoT network, by working to send large amounts of data packets into the destination network. In this Final Project (TA) research, the author tries to analyze the Support Vector Machine (SVM) and Artificial Neural Network (ANN) machine learning models to detect DoS attacks on IoT networks using Intrusion Detection System (IDS). Detecting attacks on IoT networks can be done by checking for irregularities that occur on a network. This method is an Intrusion Detection System (IDS) model, in several studies it has been proven that using the SVM and ANN models get high results for detecting DoS attacks using IDS with an accuracy value of 99% for ANN and 98% for SVM. In another study using the NSL KDD dataset, KDD 99 but in this TA using a dataset with the MQTT protocol, with this dataset the SVM model gets 92% results and 94% for ANN.

Keywords: ***iot, ids,ml.***