ABSTRACT

The potential for cyber attacks against Internet of Things (IoT) technology is enormous. Various kinds of attacks that cause disruption in the communication process include the mirai botnet attack. To detect and identify anomalies in the IoT network, the machine learning method was chosen using three algorithms that function to classify mirai botnet attacks, namely Random Forest, K-Nearest Neighbor and Decision Tree with parameters accuracy, precision, recall, and AUC. The test was carried out three times with different k-fold values. From tests 1, 2 and 3, the Random Forest, K-Nearest Neighbor, and Decision Tree algorithms produce an average value for the accuracy, precision, and recall parameters, there is no significant difference because they are close to 100%. However, for the AUC parameter, the K-Nearest Neighbor algorithm gets the highest score, with an average value of 1,000 which shows that it is superior to the Random Forest and Decision Tree algorithms.

Keywords: IoT, Mirai Botnet, Machine Learning (ML), Random Forest, K-Nearest Neighbor (KNN), Decision Tree