**Abstract**

IoT (Internet of Things) technology makes our daily life easier without realizing it. With IoT, we can monitor, manage a device remotely using the internet. Because IoT devices can be controlled remotely using the internet, this makes them vulnerable to attack by other parties. In recent years, many parties have researched detecting attacks on IoT devices using machine learning. One of the attacks that usually attack IoT devices is Distributed Denial of Service or DDoS. This kind of intrusion capable disabling network system on an IoT devices connected with flooding network traffic with large volumes of packets and continuously. To solve the problem above, this research was carried out by comparing machine learning algorithms in detecting DDoS. this study used method Naive Bayes, SVM, and Random Forest machine learning classification algorithm. In addition to measuring the model created, a DDoS attack simulation is carried out to use the data in a machine learning model. By using a third-party dataset, the three algorithms get the following results: 1. Naive Bayes accuracy 89%, f1 score 76%. 2. SVM 94% accuracy, f1 score 83%. 3. Random Forest 99% accuracy, f1 score 99%. The results of the model using the simulation data are as follows: 1. Naive Bayes accuracy 99%, f1 score 99%. 2. SVM 95% accuracy, f1 score 97%. 3. Random Forest 99% accuracy, f1 score 99%.

**Keywords:** IoT, Machine learning, DDoS, Naive Bayes, SVM, Random Forest