Abstrak
Teknologi IoT (Internet of Things) mempermudah keseharian kita tanpa disadari. Dengan IoT kita dapat memantau, mengatur suatu perangkat dari kejauhan dengan menggunakan internet. Karena perangkat IoT dapat dikendalikan dari jarak jauh menggunakan internet maka hal ini membaut perangkat tersebut rentan untuk diserang pihak lain. Beberapa tahun terakhir banyak pihak yang meneliti tentang mendeteksi serangan pada perangkat IoT menggunakan machine learning. Salah satu serangan yang biasa menyerang perangkat IoT ialah *Distributed Denial of Service* (DDoS). jenis serangan ini dapat melumpuhkan sistem jaringan pada sebuah perangkat IoT yang terhubung dengan cara membanjiri trafik jaringan dengan paket yang bervolume besar dan secara terus menerus. Untuk menyelesaikan masalah diatas maka dilakukan penelitian ini yakni dengan membandingkan algoritma machinie learning dalam mendeteksi DDoS. Metode yang digunakan dalam penelitian ini ialah algoritma klasifikasi machine learning Naive bayes, SVM, dan Random Forest. Selain itu untuk mengukur model yang dibuat dilakukan simulasi serangan DDoS untuk digunakan datanya kedalam model machine learning. Dengan menggunakan dataset pihak ketiga ketiga algoritma mendapatkan hasil sebagai berikut: 1. Naive Bayes akurasi 89%, f1 score 76%. 2. SVM akurasi 94%, f1 score 83%. 3. Random Forest akurasi 99%, f1 score 96%. Hasil model dengan menggunakan data hasil simulasi sebagai berikut:1. Naive Bayes akurasi 99%, f1 score 99%. 2. SVM akurasi 95%, f1 score 97%. 3. Random Forest akurasi 99%, f1 score 99%.

Kata kunci : IoT, Machine learning, DDoS, Naive Bayes, SVM, Random Forest