Abstrak

***Internet of Things* (IoT) merupakan sebuah alat yang mampu berkomunikasi dan mengirimkan data melalui jaringan dengan tanpa adanya campur tangan dan interaksi dari manusia. Seiring dengan berkembangnya jaman, penggunaan teknologi informasi semakin banyak dimanfaatkan dan hal ini berpengaruh terhadap kebutuhan terhadap perangkat IoT yang membuat perangkat ini semakin lama semakin berkembang luas penggunaannya. Dalam perkembangannya, masalah pada bidang privasi dan keamanan menjadi salah satu hal yang berbahaya dan harus menjadi fokus utama. Contoh serangan yang bisa menyerang perangkat IoT yakni *dictionary attack*, DDoS, mitm, dsb. Langkah yang bisa dilakukan untuk menghindari serangan tersebut adalah dengan menggunakan *Intrusion Detection System* (IDS). Tujuan dari penelitian ini adalah bagaimana mencari model yang paling optimal untuk mendeteksi serangan *dictionary attack* dan DDoS dengan menggunakan metode algoritma *machine learning* (ML) naïve bayes pada *Internet of Things* (IoT) yang disimulasikan menggunakan node red. Algoritma naïve bayes dipilih karena *Intrusion detection system* (IDS) membutuhkan tingkat performansi yang cepat dan akurasi yang tinggi. Hasil dari penelitian ini berupa model yang optimal yang dibangun dengan algoritma *machine learning* naïve bayes yang bisa diterapkan untuk *Intrusion detection system* (IDS) pada *Internet of Things* (IoT) dengan hasil akurasi untuk dataset yang diambil pada penelitian ini 99.30% untuk DDoS dan untuk *dictionary attack* 99.74% sedangkan untuk dataset yang diambil dari penelitian [19[20] untuk DDoS 82.38% dan untuk *dictionary attack* 79.88%.**

Kata kunci : IoT, IDS, *dictionary attack*, DDoS, naïve bayes.