Abstrak

***Internet of Things* (IoT) merupakan sebuah jaringan antar perangkat komputasi yang memiliki kemampuan untuk mengirim data melalui jaringan tanpa membutuhkan interaksi manusia. IoT memiliki manfaat untuk mempermudah pekerjaan manusia, tetapi di sisi lain IoT juga memiliki kelemahan yaitu rentan terkena *cyber attacks*. *Denial of Service* (DoS) merupakan salah satu serangan yang sering terjadi di dalam jaringan IoT, dengan cara kerja mengirim paket data dalam jumlah besar ke dalam jaringan yang dituju. Dalam penelitian Tugas Akhir (TA) ini, penulis mencoba melakukan analisis model pembelajaran mesin *Support Vector Machine* (SVM) dan *Artificial Neural Network* (ANN) untuk mendeteksi serangan DoS pada jaringan IoT menggunakan *Intrusion Detection System (IDS)*. Mendeteksi serangnan pada jaringan IoT dapat dilakukan dengan cara memeriksa penyimpangan yang terjadi pada sebuah jaringan. Metode tersebut merupakan model *Intrusion Detection System* (IDS), dalam beberapa penelitian membuktikan bahwa menggunakan model SVM dan ANN mendapatkan hasil yang tinggi untuk mendeteksi serangan DoS menggunakan IDS dengan nilai akurasi yang didapat 99% untuk ANN dan 98% untuk SVM. Dalam penelitian lain menggunakan dataset NSL KDD,KDD 99 namun dalam TA ini menggunakan dataset dengan protokol MQTT, dengan dataset tersebut model SVM mendapatkan hasil 92% dan 94% untuk ANN.**

Kata kunci :iot, ids,ml.