1. Pendahuluan

Latar Belakang

Dalam beberapa dekade terakhir perangkat IoT (*Internet of Things*) telah berkembang secara signifikan dan segala kegiatan manusia tidak luput dari perangkat IoT [1]. Dengan penggunaan perangkat IoT disetiap aktifitas dapat membuat pekerjaan semakin mudah, seperti penggunaan dibidang peralatan rumah tangga. Perangkat IoT seperti lampu, remot, cctv yang terhubung dengan pemilik rumah menggunakan internet sehingga dapat menjadikan rumah tersebut menjadi *Smart Home* karena pengguna dapat mengatur segala sesuatu yang ada di rumah tersebut melalui perangkat smartphone. Untuk mengimplementasikan IoT di bidang kesehatan selain bisa digunakan untuk memantau pasien dari jarak jauh tapi juga bisa untuk mengelola obat secara langsung. Penggunaan perangkat IoT sudah beredar luas dan hampir di semua bidang kehidupan, perangkat IoT mengalami peningkatan dalam jumlah penggunaannya dua kali lipat pembiayaanya pada tahun 2015 dan menghabiskan biaya sebanyak 6 triliun per tahun [2].

Bidang keamanan dan privasi merupakan kunci dari kenyamanan penggunaan perangkat IoT yang dibangun, dengan sifat IoT yang dapat dikonfigurasi secara manual membuat perangkat tersebut rentan terhadap berbagai serangan, serangan dari dalam maupun dari luar [3]. Penyerang dapat membahayakan keamanan dan privasi pengguna yang digunakan untuk mencuri akses pribadi dari penggunanya yang berguna untuk menghasilkan uang. Hal tersebut merupakan faktor lambatnya perkembangan dalam bidang keamanan dan privasi pada jaringan IoT. *Denial of Service* (DoS) merupakan sebuah bencana pada jaringan IoT jika si penyerang menargetkan pada jaringan IoT berskala kecil [3]. Contoh DoS juga mempengaruhi berbagai pada jaringan kecil seperti *smart home*, rumah sakit dan lainnya. DoS dapat membahayakan nyawa orang lain jika serangan tersebut terjadi di dalam perangkat rumah sakit yang mengakibatkan telatnya perangkat IoT untuk menampilkan informasi yang dibutuhkan. Perangkat IoT lainnya yang rentan terhadap serangan DoS contohnya *smart television, smart door locks,* dan sebagainya [3].

Dengan masalah sebagai berikut, mengamankan perangkat dari serangan DoS merupakan salah satu langkah penting untuk melindungi keamanan dan privasi pengguna, oleh karena itu berdasarkan beberapa penelitian lain masalah tersebut bisa diatasi dengan *Intrusion Detection System* (IDS) [3]. IDS merupakan sebuah metode untuk mendeteksi serangan yang mana, IDS sendiri terbagi menjadi tiga tipe berdasarkan metode deteksi yaitu *signature*, *anomaly* dan *spesification*. IDS berbasis *signature* dilakukan dengan cara menyamakan pola *traffic* normal pada jaringan dengan pola serangan (*signature*) yang sudah disimpan dalam database. Jika terdapat kesamaan dalam pola serangan yang terdapat dalam database,maka dapat dikatakan bahwa jaringan IoT tersebut sedanng terkena serangan. IDS berbasis *signature* memiliki akurasi tinggi dan tingkat *false alarm rate* yang rendah IDS berbasis *specification* dilakukan dengan mencari kesamaan pola lalu lintas (parameter) dengan kumpulan aturan dan nilai (spesifikasi) yang telah ditentukan sebelumnya untuk mendeteksi aktivitas berbahaya. Spesifikasi ini ditentukan secara manual oleh pakar keamanan. Berbeda dengan IDS berbasis *signature* dan *specification*, IDS berbasis anomali dilakukan dengan cara selalu memeriksa lalu lintas jaringan untuk setiap penyimpangan dari profil jaringan normal. Jika penyimpangan melebihi ambang batas, alarm dibunyikan untuk menandakan deteksi serangan [3] [4].

Profil jaringan normal dapat dipelajari menggunnakan algoritma *Machine Learning* (ML). IDS berbasis *anomaly* lebih sering digunakan dalam penelitian lain untuk mendeteksi serangan pada sebuah jaringan IoT, dimana IDS berbasis *anomaly* memiliki keunggulan daripada tipe lainnya yaitu memiliki tingkat efektivitas yang tinggi dalam mendeteksi serangan menggunakan ML [3]. Algoritma ML yang digunakan pada TA ini adalah *Support Vector Machine* (SVM) dan *Artificial Neural Network* (ANN), karena dalam penelitian menggunakan metode SVM selain karena memiliki performa yang efisien metode tersebut juga menghasilkan nilai akurasi sebsar 98% untuk mendeteksi seragnan DoS pada jaringan IoT menggunakan dataset NSL-KDD [5]. Sedangkan untuk metode ANN memiliki nilai akurasi yang lebih tinggi daripada SVM sebesar 99% menggunakan dataset KDD99 [6]. Dataset yang digunakan dalam TA ini adalah dataset dengan protokol MQTT, dimana MQTT merupakan sebuah protokol yang biasanya digunakan dalam jaringan IoT. Dataset tersebut mengandung 94.625 frame data yang terbagi menjadi dua yaitu jaringan dalam serangan sebanyak 45.513 dan 49.112 frame merupakan jaringan normal.

Topik dan Batasannya

Berdasarkan masalah yang diangkat di latar belakang, maka rumusan masalah untuk tugas akhir ini adalah bagaimana membangun sistem IDS dengan model *support vector machine* (SVM) dann *Artificial Neural Network* (ANN). Rumusan masalah lain yang dapat diangkat merupakan bagaimana pengaruh model SVM dan ANN terhadap akurasi pada IDS yang dihasilkan. Dari latar belakang dan rumusan masalah tersebut, tugas akhir ini memiliki batasan sebagai berikut :

1. Model *machine learning* yang diuji pada tugas akhir ini hanya *Support Vector Machine* (SVM) dan *Artifficial Neural Network* (ANN).
2. Pengujian hanya dilakukan pada dataset MQTT dan serangan yang digunakan yaitu *Denial of Service* (DoS).
3. Metriks pengujian yang digunakan adalah Akurasi, Specificity, dan Sensitivity.

Tujuan

Tujuan dari tugas akhir ini adalah membangun sebuah model optimal yang dapat mendeteksi IDS berbasis anomali dengan membandingkan performa model SVM dengan model ANN.