1. Pendahuluan

Latar Belakang

Keamanan jaringan merupakan isu yang menjadi pusat perhatian dunia di zaman sekarang ini. Perkembangan teknologi menjadi bahan penelitian agar teknologi dapat terus berkembang [1]. WSN merupakan jaringan besar dan inovatif yang terdiri dari sensor-sensor yang otomatis dan tersebar luas untuk mengumpulkan data dan mengirimkan ke database sensor sehingga data yang diperoleh dari sensor dapat menjadi dataset untuk berbagai penelitian [2]. Penggunaan WSN semakin popular untuk memudahkan berbagai aktivitas sehingga keamanannya semakin rentan berbagai ancaman. Banyak ancaman yang dapat merusak WSN salah satunya adalah serangan Denial of Service.

Serangan tersebut memiliki banyak jenis dengan tujuan yang berbeda, contohnya adalah Routing Attack. Tujuan utama dari serangan tersebut adalah menghentikan fungsi normal pada jaringan sensor dengan mengacaukan trafik seperti mengirimkan banyak paket data yang tidak dikenal sehingga menyebabkan kerusakan pada jaringan, mengurangi efisiensi kinerja jaringan, dan memblokir jaringan [4]. Routing Attack memiliki berbagai jenis antara lain Grayhole Attack yang bertujuan menggangu akses jaringan dengan memperlambat koneksi, Blackhole Attack yaitu serangan yang memblokir akses ke suatu jaringan dengan cara mengarahkan semua trafik ke alamat yang tidak valid atau biasa disebut dengan “Black Hole”, Flooding Attack bertujuan untuk menyerang server dengan cara mengirimkan permintaan paket dalam jumlah yang sangat besar kepada server sehingga server tidak dapat menangani permintaan tersebut, dan Scheduling Attack menyebabkan user tidak dapat mengakses sumber daya miliknya atau dengan kata lain melakukan pemblokiran secara berkala [5].

Intrusion Detection System (IDS) adalah sebuah sistem yang dapat memberikan peringatan mengenai suatu anomaly yang masuk kedalam sistem. Sistem deteksi ini sangat berguna untuk mengatasi berbagai jenis Routing Attack [6]. Model machine learning juga dapat digunakan sebagai alat bantu untuk menentukan apakah data yang didapatkan merupakan suatu serangan atau bukan dengan menggunakan metode klasifikasi pada data tersebut. Metode klasifikasi bertujuan untuk melihat keakuratan data dan menghasilkan nilai akurasi dari model machine learning yang digunakan, semaking besar nilai akurasinya maka semakin baik model tersebut dalam mengidentifikasi serangan [7]. Selain menggunakan metode klasifikasi, model machine learning dapat melihat data tersebut merupakan serangan atau bukan dengan menggunakan metode false alarm rate, dimana jika nilai false alarm rate rendah maka nilai akurasi terbukti mengidentifikasi data tersebut sebagai serangan [8]. Library Scikit-learn merupakan library pada bahasa python yang sering digunakan untuk penelitian machine learning. Library ini memiliki berbagai algoritma dan fungsi, seperti data preprocessing, pemodelan machine learning, dan evaluasi kinerja [9].

Selanjutnya, penelitian ini mengimplementasikan pemisahan data pada dataset yang digunakan. Dataset dipecah menjadi tiga bagian, antara lain data training, data testing, dan data validasi. Pemisahan data tersebut bertujuan untuk mengetahui nilai akurasi dari model machine learning, apakah hasil dari penggunaan data validasi dan data testing menunjukan nilai yang sama atau berbeda [10]. Perbandingan dari kedua data yang digunakan tersebut diharapkan dapat lebih akurat dalam mengidentifikasi Routing Attack.

Penelitian ini menggunakan model machine learning Decision Tree, Naïve Bayes, Support Vector Machine, dan K-Neirest Neighbour dengan tujuan untuk mengetahui model mana yang terbaik dalam menghasilkan nilai akurasi dan nilai false alarm rate. Jika nilai akurasi model tinggi dan nilai false alarm rate rendah, model tersebut baik digunakan untuk mengidentifikasi Routing Attack pada data. Pada akhir penelitian ini, model machine learning yang memiliki hasil terbaik merupakan model yang sangat optimal untuk penelitian seperti ini

Topik dan Batasannya

Topik dari penelitian ini adalah bagaimana mengimplementasikan dan membandingkan manakah model machine learning (DT, NB, SVM, dan KNN) yang terbaik untuk mengidentifikasi Routing Attack dilihat dari nilai akurasi dan nilai false alarm rate dengan membagi dataset menjadi tiga bagian (data training, data testing, dan data validasi).

Terdapat juga batasan masalah pada penelitian ini meliputi penggunaan tools google collab dan bahasa pemrogramman python untuk implementasi codenya, model machine learning yang digunakan hanya empat (DT, NB, SVM, dan KNN), dataset penelitian ini dipisah menjadi tiga bagian (data training, data testing, dan data validasi), dan parameter pada penelitian ini ada tiga meliputi akurasi, false alarm rate, dan processing time.

Tujuan

Tujuan dari penelitian ini untuk mengetahui model machine learning mana yang terbaik untuk mengidentifikasi Routing Attack pada dataset WSN-DS, dan untuk mengetahui apakah dengan membagi dataset

menjadi tiga bagian (data training, data testing, data validasi) mempengaruhi hasil nilai akurasi dari model yang digunakan.

Organisasi Tulisan

Struktur penulisan dalam penelitian ini sebagai berikut: Bab 1 merupakan Pendahuluan yang membahas konteks penelitian dan kondisi pengetahuan saat ini. Bab 2 merupakan Studi Terkait yang menjelaskan hasil dari penelitian sebelumnya dan perbedaan penelitian ini dengan penelitian lain. Bab 3 merupakan Sistem yang dibangun yang menjelaskan tentang rancangan model dan sistem yang pada penelitian ini. Bab 4 merupakan Evaluasi yang membahas terkait hasil dari penelitian ini, dan Bab 5 adalah kesimpulan dari penelitian ini.