

## **1. Pendahuluan**

### **Latar Belakang**

Seiring dengan berkembangnya internet dan teknologi, lingkungan sekitar kita berkembang menjadi lingkungan yang penuh dengan smart-computing. Perkembangan pesat termasuk perkembangan keamanan jaringan network. Meskipun demikian, serangan-serangan yang terjadi pada jaringan network juga terus berkembang. Salah satu serangan tersebut adalah DoS. DoS merupakan serangan yang menyebabkan komputer atau device tidak berfungsi dengan normal. Serangan ini bisa dideteksi dengan metode IDS atau Intrusion Detection System. IDS memiliki fungsi untuk mendeteksi setiap aktivitas pada jaringan yang tidak normal.

Namun karena IDS memiliki tingkat akurasi yang tidak akurat dan memiliki waktu lama untuk mendeteksinya, maka ditambahkan algoritma-algoritma yang membantu untuk masalah ini. Salah satunya adalah dengan menggunakan algoritma Relevance vector machine atau RVM. RVM adalah algoritma pembelajaran mesin yang diadaptasi dari Bayesian Framework. Dari Bayesian Framework tersebut, user dapat mengetahui distribusi probabilitas pada nilai parameter dari suatu model atau classifier sehingga menghasilkan model design IDS yang lebih baik dibandingkan dengan SVM. Relevance vector machine memiliki performa generalisasi yang lebih baik dibandingkan dengan SVM karena memiliki support vector yang lebih sedikit [1].

Banyak metode yang telah digunakan untuk mendeteksi serangan DoS dengan algoritma-algoritma diantaranya Naïve Bayes [2], Deep Learning [3], Decision Tree [4], dan lain-lain. Untuk penelitian ini, peneliti menggunakan algoritma Relevance Vector Machine untuk mengetahui nilai akurasi algoritma ini dalam mendeteksi serangan DoS.

### **Topik dan Batasannya**

Berdasarkan latar belakang, rumusan masalah yang dibahas pada penelitian adalah nilai akurasi dari algoritma Relevance Vector Machine dalam mendeteksi DoS dari dataset NSL-KDD. Nilai akurasi tersebut didapat dari

Batasan masalah pada penelitian ini adalah dataset yang digunakan merupakan dataset NSL-KDD, Bahasa pemrograman yang digunakan adalah python 3 atau lebih. Library yang digunakan adalah sklearn-rvm untuk mengaplikasikan algoritma Relevance Vector Machine. Aplikasi yang digunakan adalah Jupyter Notebook. Jumlah data yang akan digunakan dalam training adalah berjumlah 1000 data.

### **Tujuan**

Tujuan dari tugas akhir ini berdasarkan rumusan masalah tersebut adalah untuk mendapatkan nilai akurasi algoritma Relevance Vector Machine dalam mendeteksi serangan DoS dengan menggunakan dataset NSL-KDD.

### **Organisasi Tulisan**

Setelah bagian pendahuluan yang telah dipaparkan, dalam penelitian ini disusun dalam beberapa bab yang terdiri dari Studi terkait, Sistem yang dibangun, Evaluasi, dan Kesimpulan.