BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era perkembangan teknologi saat ini, internet telah menjadi kebutuhan penting dalam berbagai aspek kehidupan manusia saat ini. Kemajuan teknologi informasi dan komunikasi (TIK) yang semakin pesat, membuat aktivitas sehari-hari masyarakat kini semakin banyak dilakukan dengan menggunakan internet yang menyebabkan peningkatan lalu lintas jaringan. Dikarenakan TIK menjadi bagian penting dari kehidupan modern, terdapat berbagai jenis serangan dan variasinya yang terus berkembang. Salah satu jenis serangan DoS (*Denial of Service*) adalah DDoS (*Distributed Denial of Service*), dimana penyerang memanfatkan komputer yang telah terinfeksi untuk mengirimkan paket dalam jumlah besar. Serangan DDoS menjadi salah satu metode yang paling sering digunakan oleh *hacker* untuk melumpuhkan sebuah *server*. Sampai saat ini serangan DDoS tetap menjadi jenis ancaman utama dalam keamanan *cyber*[1].

Metode tradisional dalam mendeteksi serangan DDoS seperti *rule-based detection* memiliki keterbatasan dalam mengidentifikasi pola baru atau serangan yang belum pernah terjadi sebelumnya. Dalam beberapa tahun terakhir, teknologi *Machine Learning* (ML) telah muncul sebagai solusi inovatif dalam deteksi serangan siber. *Machine Learning* mampu menganalisis pola trafik jaringan dengan lebih adaptif dan mampu mengenali pola-pola *anomali* yang mengindikasikan adanya serangan[2]. Oleh karena itu, penelitian ini melakukan komparasi dua algoritma yaitu *K-Nearest Neighbor* dan *Support Vector Machine* untuk melihat algoritma mana yang memiliki perfoma terbaik dalam mendeteksi serangan DDoS.

KNN adalah metode untuk melakukan klasifikasi terhadap objek yang di uji berdasarkan data yang jaraknya paling dekat dengan objek tersebut. SVM adalah sebuah algoritma yang menggunakan pemetaan nonlinear untuk mengubah data pelatihan dari dimensi aslinya ke dimensi yang lebih tinggi. Dalam penelitian

tentang Perbandingan Algoritma SVM dan KNN dalam Menghasilkan Klasifikasi DDoS dan *Benign,* SVM mendapatkan akurasi 90,75% sedangkan KNN mendapatkan akurasi 95,50%[3]. Penelitian lainnya tentang Optimalisasi Deteksi Serangan DDoS Menggunakan Algoritma Random Forest, SVM, KNN dan MLP pada Jaringan Komputer menunjukkan bahwa hasil akurasi algoritma *support vector machine* sebesar 98,37%, *K-nearest neighbor sebesar* 99% sudah cukup baik dalam mendeteksi serangan[4].

Semakin meningkatnya serangan *Distributed Denial of service* (DDoS) yang sulit dideteksi karena pola lalu lintasnya seperti trafik normal. Sehingga kesulitan dalam mendeteksi dan mengklasifikasikan serangan *Distributed Denial of Service* (DDoS) secara akurat. Serangan DDoS yang semakin kompleks dapat menyebabkan gangguan layanan, penurunan kinerja sistem, dan kerugian bagi pengguna serta penyedia layanan. Dengan menggunakan algoritma *K-Nearest Neighbors* (KNN) *dan Support Vector Machine* (SVM), diharapkan dapat menjadi solusi dalam mengidentifikasi pola trafik yang mencurigakan dan meningkatkan akurasi deteksi serangan.

Berdasarkan persoalan diatas, peneliti tertarik untuk mengambil penelitian yang berjudul "Klasifikasi Serangan DDoS Menggunakan Algoritma KNN dan SVM. Solusi dari permasalahan tersebut adalah mengembangkan sistem deteksi berbasis *Machine Learning* dengan menggunakan algoritma *K-Nearest Neighbor* (KNN) dan *Support Vector Machine* (SVM) yang dapat menganalisis pola trafik jaringan yang mencurigakan secara akurat dalam mendeteksi serangan DDoS.

1.2 Rumusan Masalah

Dengan latar belakang yang sudah di uraikan, maka pentingnya suatu persoalan harus dipecahkan pada proses ini:

1. Seberapa tinggi *accuracy, precision, recall* dan *f1-score* pada algoritma KNN dalam mendeteksi serangan DDoS?
2. Seberapa tinggi *accuracy, precision, recall* dan *f1-score* pada algoritma

SVM dalam mendeteksi serangan DDoS?

3. Algoritma manakah yang paling efektif dalam mendeteksi serangan DDoS?

1.3 Batasan Masalah

Supaya masalah yang akan diangkat tidak menyebar luas, tentunya menghasilkan batasan masalah yaitu:

1. Pembatasan pada jenis dan ketersediaan data yang digunakan dalam analisis.
2. Algoritma yang digunakan hanya mencakup KNN dan SVM tanpa membandingkan dengan algoritma lain.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengevaluasi performa algoritma KNN dan SVM dalam mendeteksi serangan DDoS.
2. Mengukur efektivitas *accuracy, precision, recall,* dan *f1-score* diantara algoritma KNN dan SVM dalam mendeteksi serangan DDoS.

1.5 Manfaat Penelitian

Berikut ini adalah manfaat penelitian baik secara teoritis dan praktis:

1. Memberikan pengetahuan terkait akurasi KNN dan SVM dalam klasifikasi data serangan.
2. Mengembangkan model deteksi dan algoritma berbasis *Machine Learning* yang lebih efisien dan akurat untuk mendeteksi serangan DDoS.
3. Menjadi referensi dalam mengembangkan sistem deteksi keamanan dalam mencegah serangan-serangan DDoS.
4. Membantu dalam mencegah gangguan layanan dan mengurangi risiko serangan DDoS pada infrastruktur jaringan.

1.6 Sistematika Penulisan

Dalam penulisan ini menghasilkan sesuatu sistematika yang bertujuan sebagai gambaran ringkas dari bab-bab yang mencakup hal yang berkaitan sebagai berikut:

BAB I PENDAHULUAN, bab ini menjelaskan latar belakang, perumusan masalah, batasan masalah, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, bab ini mencakup tinjauan hasil pustaka dan dasar teori, tinjauan pustaka akan membahas mengenai uraian tentang kajian berbagai macam pustaka yang kemudian hasil dari kajian ini digabungkan dengan masalah yang sedang diteliti dalam proses penyusuanan skripsi.

BAB III METODE PENELITIAN, pembahasan ini berkaitan tentang penyampaian mengenai bahan dan peralatan yang akan digunakan dalam melakukan penelitian, serta metode dan perancangan sistem yang meliputi kebutuhan dalam membuat sistem deteksi serangan.

BAB IV HASIL DAN PEMBAHASAN, uraian pada bab ini berisikan tentang pengembangan tahapan pembuatan sistem, penerapan algoritma, pengujian, mengevaluasi efektivitas kinerja dalam mendeteksi serangan.

BAB V PENUTUP, pada bab ini menyampaikan hasil akhir dari penyampaian pada bab-bab yang sudah tertera, kemudian dari hasil tersebut penulis menyampaian beberapa saran yang bermanfaat untuk menambah sesuatu yang kurang supaya menjadi lengkap pada proses tersebut.