

# **BAB I**

## **PENDAHULUAN**

### **I.1 Latar Belakang**

Kemajuan teknologi adalah sesuatu yang tidak bisa dihindari dalam kehidupan ini, karena kemajuan teknologi akan berjalan sesuai dengan kemajuan ilmu pengetahuan. Seiringnya berkembang pesat adanya teknologi, yaitu diiringi dengan adanya pesat jumlah user dan hardware yang menciptakan jaringan konvensional bersifat tidak fleksibel dan efisien untuk diintegrasikan dengan jaringan terbaru. Dalam operasinya, jaringan tradisional juga tidak mudah diprogram ulang. Hal ini membuat para peneliti mengembangkan sebuah teknologi baru yang membuat jaringan terintegrasi dan berbasis software (Sanubari et al., 2020). Adapun dalam jaringan konvensional router menerapkan semua algoritma routing dan memutuskan bagaimana proses forwarding suatu paket (Chris et al., 2019). Namun seiring berkembangnya teknologi tersebut terdapat ancaman keamanan jaringan yang semakin banyak jenisnya.

Software Define Network (SDN) berbasis software adalah istilah yang merujuk pada paradigma baru dalam mendesain, mengelola dan mengimplementasikan jaringan, terutama untuk mendukung kebutuhan dan inovasi di bidang ini semakin waktu yang lama semakin kompleks. Konsep pada SDN adalah dengan melakukan pemisahan eksplisit antara control dan forwarding plane, serta kemudian melakukan abstraksi sistem dan mengisolasi kompleksitas yang ada pada komponen atau sub-sistem dengan mendefinisikan antar-muka (interface) yang standard (Aziiz Burhanudin Faidzin Labay et al., 2021)

Salah satu ancaman terbesar yang dihadapi oleh jaringan komputer adalah serangan Distributed Denial of Service (DDoS). DDoS adalah serangan terdistribusi yang bertujuan untuk menguras

bandwidth atau mengganggu ketersediaan sumber daya korban dengan membanjiri server, tautan jaringan dan perangkat jaringan dengan lalu lintas yang tidak sah (Chris et al., 2019). Serangan DDoS saat ini sering menargetkan layanan tertentu sehingga aplikasi yang diserang mengalami gangguan sementara komponen jaringan lain seperti link, switch, dan router tetap berfungsi normal. Adapun serangan ini dapat menyebabkan gangguan terhadap ketersediaan layanan, mengakibatkan kerugian finansial bagi organisasi yang terkena dampaknya.

Dalam upaya untuk mengatasi masalah ini maka dapat dimanfaatkan teknologi berbasis metode machine learning maka sistem dapat belajar dari data lalu lintas jaringan yang ada dan mengidentifikasi pola-pola yang menunjukkan adanya serangan. Salah satu algoritma machine learning yang efektif adalah Support Vector Machine (SVM) yaitu sebuah untuk mengklasifikasikan data dengan mencari hyperplane terbaik yang sehingga memisahkan kelas dari serangan maupun non-serangan. Berdasarkan permasalahan diatas maka peneliti akan mengembangkan sistem untuk mendeteksi adanya serangan DDoS pada arsitektur SDN menggunakan algoritma *support vector machine*. Dengan adanya penelitian ini diharapkan dapat membuat sistem deteksi serangan DDoS yang dapat mengidentifikasi serangan dengan mengklasifikasikan lalu lintas jaringan menggunakan model *Support Vector Machine*.

## **I.2 Perumusan Masalah**

Rumusan permasalahan dari penelitian adalah sebagai berikut.

1. Bagaimana membangun sistem deteksi serangan DDoS pada jaringan *software defined Network (SDN)* dengan machine learning menggunakan *Support Vector Machine (SVM)*?
2. Bagaimana kinerja *Machine learning* model algoritma SVM dalam melakukan klasifikasi serangan DDoS?

### **I.3 Tujuan Tugas Akhir**

Tujuan permasalahan dari penelitian adalah sebagai berikut.

1. Pengujian kinerja serangan DDoS menggunakan *machine learning* model algoritma SVM.
2. Mengetahui hasil sistem deteksi serangan DDoS pada jaringan SDN dengan *Machine learning* menggunakan SVM.

### **I.4 Batasan Tugas Akhir**

Batasan tugas akhir ini adalah sebagai berikut:

1. Pengujian pada jaringan lokal menggunakan Ubuntu versi 22.04
2. Deteksi *Distributed denial of Service* (DdoS) secara real time.
3. Tipe serangan DDoS menggunakan Hping3 dengan ICMP Attack

### **I.5 Manfaat Tugas Akhir**

Manfaat tugas akhir ini:

1. Bagi peneliti, Penelitian ini akan bermanfaat dalam mendalami ilmu serta pengetahuan tentang sistem deteksi serangan DDoS pada SDN
2. Bagi peneliti lain, Penelitian ini dapat dijadikan sebagai referensi untuk penelitian yang lebih lanjut menggunakan metode algoritma SVM.
3. Bagi Universitas Telkom, Peneliti ini bermanfaat dalam meningkatkan segi keamanan jaringan untuk mengantisipasi berbagai serangan yang ada.

### **I.6 Sistematika Penulisan**

Tugas akhir ini diuraikan dengan sistematika penulisan sebagai berikut:

#### **Bab I      Pendahuluan**

Pada bab ini berisi uraian mengenai konteks permasalahan, latar belakang permasalahan, perumusan masalah yang bertujuan untuk menyelesaikan masalah dengan menciptakan sistem terintegrasi yang terdiri dari manusia dengan material dan/atau peralatan/mesin dan/atau informasi dan/atau energy, batasan tugas akhir, manfaat tugas akhir, dan sistematika penulisan.

## **Bab II Tinjauan Pustaka**

Bab ini berisi literatur yang relevan dengan permasalahan yang diambil dan dibahas pula hasil-hasil referensi buku/ penelitian/ referensi lainnya yang dapat digunakan untuk merancang dan menyelesaikan masalah. Minimal terdapat lebih dari satu metodologi/metode/kerangka kerja yang disertakan pada bab ini untuk menyelesaikan permasalahan atau meminimalisir gap antara kondisi eksisting dengan target. Pada akhir bab ini, analisis pemilihan metodologi/metode/kerangka kerja harus dijelaskan untuk menentukan metodologi/metode/kerangka kerja yang akan digunakan di tugas akhir ini.

## **Bab III Metodologi Penyelesaian Masalah**

Metodologi penyelesaian merupakan penjelasan metode / konsep / kerangka kerja yang telah dipilih pada bab Tinjauan Pustaka. Pada tugas akhir Pada bab ini dijelaskan langkah-langkah tugas akhir secara rinci meliputi: tahap merumuskan masalah, merumuskan hipotesis, mengembangkan model, mengidentifikasi dan melakukan operasionalisasi variabel, menyusun kuesioner, merancang pengumpulan dan pengolahan data, melakukan uji instrumen, merancang analisis pengolahan data dalam rangka perancangan sistem terintegrasi untuk penyelesaian permasalahan.

## **Bab IV Perancangan Sistem Terintegrasi**

Seluruh kegiatan dalam rangka perancangan sistem terintegrasi untuk penyelesaian masalah dapat ditulis di bab ini. Kegiatan yang dilakukan dapat berupa pengumpulan dan pengolahan data, pengujian data, dan perancangan solusi.

## **Bab V Analisa Hasil dan Evaluasi**

Pada bab ini, disajikan hasil rancangan, temuan, analisis dan

pengolahan data. Selain itu bab ini juga berisi tentang validasi atau verifikasi hasil dari solusi, sehingga hasil tersebut apakah telah benar-benar menyelesaikan masalah atau menurunkan gap antara kondisi eksisting dan target yang akan dicapai. Analisis sensitivitas juga dapat digunakan di bab ini untuk lebih mengetahui hasil tugas akhir dapat diterapkan baik secara khusus di konteks tugas akhir maupun secara umum di konteks serupa (misal perusahaan di sektor serupa). Selain itu metode-metode evaluasi yang lain dapat di terapkan untuk memvalidasi hasil sesuai dengan kebutuhan.

Secara keseluruhan bab ini membahas secara mendetail mengenai hasil dari pengerjaan solusi dan refleksinya terhadap tujuan tugas akhir. Untuk tugas akhir yang berfokus pada merancang sistem informasi/ aplikasi maka penamaan bab ini mengikuti tahapan penerapan SDLC yang digunakan dalam tugas akhir.

## **Bab VI      Kesimpulan dan Saran**

Pada bab ini dijelaskan kesimpulan dari penyelesaian masalah yang dilakukan serta jawaban dari rumusan permasalahan yang ada pada bagian pendahuluan. Saran dari solusi dikemukakan pada bab ini untuk tugas akhir selanjutnya.