BAB I PENDAHULUAN

I.1. Latar Belakang

Pada masa sekarang ini jaringan telah menjadi infrastruktur yang sangat penting bagi bisnis, perkantoran maupun kampus. Jaringan lokal atau sering disebut *Local Area Network* (LAN) juga sangat cocok untuk diimplementasikan pada area tersebut. Oleh karena itu, sangat penting sekali untuk memiliki sistem infrastruktur jaringan yang mudah dikelola namun memiliki kemampuan kerja yang optimal dan juga fleksibel. Namun jaringan komputer merupakan sesuatu yang kompleks dan sulit untuk dikelola. Banyak alat yang diperlukan untuk merancang dan mengelola jaringan komputer, mulai dari *router* dan *switch* hingga ke *middlebox* seperti *firewall*, *translator* alamat jaringan, dan banyak lagi.

Berdasarkan fakta-fakta yang telah disebutkan, arsitektur jaringan seperti itu sudah tidak lagi cocok dengan kebutuhan *enterprise*, *carriers* dan *end user* saat ini. Untuk mengatasi masalah tersebut, berkembanglah paradigma jaringan baru yang disebut dengan *Software Defined Network* (SDN).

Software Defined Network (SDN) atau jaringan berbasis *software* adalah sebuah teknologi jaringan atau paradigma baru yang dikembangkan oleh para peneliti yang memungkinkan administrator jaringan untuk memiliki kontrol pada trafik jaringan, dimana *data plane* dikontrol oleh *control plane* yang bersifat *remote* dan tidak lagi terikat dalam perangkat jaringan (Tulloh, 2017). Jadi dengan SDN, seorang admin dapat mengendalikan *data flow* karena sifatnya yang terpusat.

Karena SDN adalah sebuah jaringan yang dapat dijalankan secara terbuka oleh siapa saja, membuat jaringan SDN rentan terhadap serangan terutama pada bagian *control plane* dan *data plane*. Jika koneksi antara *switch* dan *controller* bermasalah atau terputus, jaringan akan kehilangan *processing plane* atau *data plane*-nya. Proses tersebut mengartikan bahwa pengiriman tidak dapat lagi berjalan di *controller*, *controller* dan arsitektur SDN akan hilang. Salah satu kemungkinan yang dapat terjadi pada *controller* yang tidak dapat dijangkau adalah dengan serangan *Distributed Denial of Service* (DDoS).

Peningkatan penggunaan paket sangat beragam di seluruh dunia sehingga dapat menyebabkan peningkatan ancaman keamanan, seperti serangan *Distributed Denial of Service* (DDoS).Tujuan utama dari serangan DDoS adalah untuk membuat server tidak dapat diakses dengan mengkonsumsi banyak sumber daya seperti *bandwith, memory* atau CPU. Masalah deteksi DDoS adalah masalah klasik di bidang sistem deteksi intrusi, oleh karena itu terdapat cara yang lengkap. Namun serangan DDoS terus menjadi salah satu ancaman *cyber* terbesar yang mempengaruhi beberapa sektor yang dapat berdampak merugikan. Pada tahun 2019 ukuran serangan DDoS meningkat 273%. Selain itu, 91% korban melaporkan bahwa serangan tersebut membuat *bandwith* internet mereka lelet (District et al., 2022).

Dalam menangani hal ini, telah dilakukan beberapa penelitian untuk dapat melakukan deteksi pada serangan tersebut. Untuk dapat melakukannya, metode yang cepat dan efektif diperlukan aktif bekerja dalam *controller* sebelum serangan terus membanjiri sistem tersebut. Pada saat yang sama, metode harus ringan untuk menghindari pemrosesan yang berlebihan dan respon cepat, khususnya pada puncak serangan. Dalam penelitian ini penulis membangun sistem deteksi dan mitigasi serangan DDoS pada jaringan SDN menggunakan *K-Nearest Neighbors* sebagai *machine learning* untuk dapat melakukan klasifikasi serangan. Serangan yang dilakukan yaitu menggunakan ICMP *Attack. Controller* pada jaringan SDN akan dikembangkan dengan diterapkan KNN yang berfungsi sebagai deteksi dan mitigasi paket serangan DDoS dengan cara menginstruksi pada *switch* untuk menginstal *flow* mitigasi DDoS. Sebelum dijalankan skenario penyerangan KNN akan melakukan pengenalan terlebih dahulu terhadap data agar dapat mengenali jika adanya penyerang, maka *controller* akan melakukan mitigasi terhadap serangan yang sudah dikenali. Sehingga pada penelitian ini diharapkan dapat berkontribusi terhadap keamanan jaringan khususnya pada jaringan SDN.

I.2. Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana membangun sistem deteksi dan mitigasi serangan *Distributed Denial of Service* (DDoS) pada jaringan *Software Defined Network* (SDN) dengan *machine learning* menggunakan *K-Nearest Neighbors*?
b. Bagaimana kinerja *Machine Learning* model algoritma KNN dalam melakukan klasifikasi serangan DDoS?

I.3. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

a. Membangun sistem deteksi dan mitigasi serangan DDoS pada jaringan SDN dengan *machine learning* menggunakan KNN.
b. Melakukan pengujian kinerja klasifikasi serangan DDoS menggunakan *machine learning* model algoritma KNN.

I.4. Batasan Penelitian

Ruang lingkup pembahasan yang digunakan dalam penelitian ini antara lain:

1. Diimplementasikan pada jaringan topologi *star*.
2. Pengujian dilakukan pada jaringan lokal.
3. Model algoritma *machine learning* yang digunakan *K-Nearest Neighbors.*
4. Formula yang digunakan dalam algortima KNN pada penelitian ini adalah *Euclidean Distance*.
5. Nilai K yang digunakan untuk melakukan klasifikasi pada penelitian ini adalah 5.
6. Tipe serangan DDoS menggunakan DDoS *ICMP Attack*.
7. Data yang digunakan dilakukan dengan *generate data*.
8. Deteksi DDoS dilakukan secara *real time.*
9. Mitigasi yang dilakukan yaitu *block port* dan *drop packet*.

I.5. Manfaat Penelitian

Adapun manfaat dari penelitian ini:

1. Memberikan informasi mengenai kelemahan dari sebuah jaringan SDN dengan celah-celah tertentu.
2. Memberikan solusi untuk dapat diterapkan jika terdapat kekurangan atau kelemahan yang terdapat dalam jaringan dengan menggunakan metodologi yang sudah dikerjakan.
3. Meminimalisir terjadinya serangan terhadap jaringan kita dengan menerapkan metode yang disarankan.