BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah mendorong evolusi arsitektur jaringan komputer menuju sistem yang lebih fleksibel dan terotomatisasi. Salah satu teknologi yang sedang berkembang pesat adalah *Software Defined Networking* (SDN), yang memisahkan antara control plane dan data plane (Shaghaghi et al., 2018). Dengan pemisahan ini, administrator jaringan dapat mengatur dan memantau seluruh perangkat jaringan dari satu titik pusat secara dinamis dan efisien. SDN memungkinkan konfigurasi jaringan yang cepat, skalabel, dan lebih adaptif terhadap perubahan serta ancaman yang mungkin terjadi di dalam jaringan (Melissa & Indriani Lestariningati, 2018). Salah satu tantangan utama dalam pengelolaan jaringan modern adalah menjaga keamanan dan ketersediaan layanan. Di antara berbagai jenis serangan yang ada, salah satunya *Denial of Service* (DoS).

DoS merupakan salah satu yang paling merugikan. Serangan ini bertujuan untuk membuat suatu layanan tidak tersedia dengan cara membanjiri sistem dengan lalu lintas yang berlebihan. Salah satu bentuk DoS yang cukup terkenal dan masih menjadi ancaman adalah *Ping of Death*, yaitu serangan yang memanfaatkan kelemahan dalam pengolahan paket *Internet Control Message Protocol (*ICMP) berukuran besar yang dapat menyebabkan sistem crash atau tidak responsif (Endah Wahanani et al., 2016) Dalam konteks jaringan SDN, ancaman seperti ini perlu dimitigasi melalui pendekatan yang lebih adaptif dan terintegrasi dengan *Controller*.

Pada penelitian ini dilakukan dengan mengambil studi kasus berupa penerapan sistem *Firewall* pada jaringan SDN yang dibangun menggunakan Mininet sebagai emulator, Ubuntu Linux sebagai sistem operasi dasar, dan *Ryu Controller* sebagai pusat kendali jaringan (Jaiswal, 2022). Sistem ini disimulasikan pada lingkungan virtual menggunakan VMware untuk memastikan fleksibilitas dalam pengujian. Serangan *Ping of Death* disimulasikan menggunakan alat hping3, dan pengaruhnya terhadap performa jaringan diukur menggunakan parameter seperti

packet loss. *Firewall* yang dirancang memiliki kemampuan mendeteksi serangan dan secara otomatis melakukan mitigasi melalui teknik *Blacklisting* terhadap alamat IP penyerang.

Metode yang digunakan dalam penelitian ini menggabungkan pendekatan pengendalian keamanan berbasis SDN dengan pembelajaran mesin menggunakan algoritma *Support Vector Machine* (SVM). Algoritma ini digunakan untuk membedakan antara *traffic* normal dan *traffic* serangan berdasarkan fitur tertentu seperti ukuran paket ICMP. Integrasi ini memungkinkan sistem *Firewall* untuk tidak hanya memfilter lalu lintas berdasarkan aturan statis, tetapi juga berdasarkan hasil klasifikasi cerdas. Sistem ini dirancang agar mampu bereaksi dalam waktu nyata terhadap pola serangan yang dikenali.

Dari rangkaian pemahaman terhadap teknologi SDN, karakteristik serangan DoS *Ping of Death*, serta pentingnya mitigasi adaptif, penulis terdorong untuk melakukan penelitian ini. Penerapan *Firewall* cerdas pada jaringan SDN diharapkan dapat menjadi solusi efektif dan efisien untuk mendeteksi serta mengurangi dampak serangan DoS, khususnya jenis *Ping of Death*. Dengan demikian, penelitian ini tidak hanya memberikan kontribusi pada penguatan sistem keamanan jaringan, tetapi juga pada pengembangan sistem adaptif berbasis pembelajaran mesin dalam lingkungan jaringan yang terprogram.

I.2 Perumusan Masalah

Berdasarkan identifikasi latar belakang permasalahan, penelitian ini mencoba menjawab pertanyaan-pertanyaan berikut:

1. Bagaimana merancang dan mengimplementasikan sistem *Firewall* berbasis SDN yang terintegrasi dengan algoritma SVM untuk mendeteksi dan memitigasi serangan *ping of death*?
2. Seberapa akurat dan efektif model klasifikasi SVM dalam mendeteksi lalu lintas serangan *ping of Death* secara *real-time*?
3. Bagaimana pengaruh penerapan *Firewall* SDN terhadap performa jaringan, ditinjau dari parameter *Round-Trip Time* pada kondisi normal dan saat terjadi serangan?

I.3 Tujuan Penelitian

Berdasarkan masalah yang terjadi maka tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Membangun sistem *Firewall* berbasis SDN yang mampu mendeteksi dan memitigasi serangan *Ping of Death* secara otomatis yang terintegrasi dengan algoritma SVM.
2. Mengevaluasi tingkat akurasi dan efektivitas model klasifikasi SVM dalam mendeteksi lalu lintas serangan *Ping of Death* secara *real-time.*
3. Menganalisis pengaruh penerapan *Firewall* SDN terhadap performa jaringan, khususnya ditinjau dari parameter *Round-Trip Time* pada kondisi normal dan ketika terjadi serangan.

I.4 Batasan Penelitian

Untuk mencapai fokus yang terarah dalam penelitian ini, ditetapkan beberapa batasan sebagai berikut:

1. Serangan yang diuji hanya terbatas pada tipe *Ping of Death* dengan variasi ukuran paket.
2. Lingkungan eksperimen dilakukan secara virtual menggunakan Mininet dan virtual machine berbasis Linux Ubuntu 22.04.

I.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan kontribusi sebagai berikut:

Aspek Teoritis:

1. Memberikan kontribusi akademik terhadap pengembangan model mitigasi serangan jaringan berbasis SDN.
2. Menambah referensi ilmiah dalam integrasi pembelajaran mesin (SVM) dengan sistem keamanan berbasis *Controller*.

Aspek Praktis:

1. Menjadi solusi alternatif yang fleksibel untuk mendeteksi dan memitigasi serangan *Ping of Death* di jaringan modern.

2. Memberikan acuan implementatif bagi administrator jaringan dalam merancang *Firewall* dinamis berbasis SDN.