BAB I PENDAHULUAN

I.1 Latar Belakang

Software-Defined Networking (SDN) merupakan inovasi dalam pengelolaan jaringan yang memungkinkan pemisahan antara lapisan kontrol dan lapisan data, memberikan fleksibilitas lebih besar dalam mengelola dan mengoptimalkan lalu lintas jaringan. Pada jaringan tradisional, fungsi kontrol dan data biasanya digabungkan dalam perangkat keras jaringan. Namun, dengan SDN, kontrol jaringan dilakukan secara terpusat melalui perangkat lunak khusus, yang membuat pengelolaan jaringan lebih mudah dan efisien. SDN memungkinkan penyesuaian terhadap kebutuhan jaringan yang terus berubah, meningkatkan fleksibilitas dalam pengaturan, konfigurasi, serta peningkatan keamanan(Irfan, n.d.).

Keunggulan utama dari SDN terletak pada pengelolaan terpusat yang memungkinkan administrator jaringan melakukan pemantauan dan pengendalian secara menyeluruh dari satu titik. Hal ini membantu dalam pemeliharaan, konfigurasi, serta penanganan masalah jaringan dengan lebih cepat. Namun, SDN juga memiliki kelemahan. Dengan adanya lapisan kontrol terpusat, SDN menjadi target rentan terhadap serangan siber, khususnya serangan yang memanfaatkan kelengahan di lapisan kontrol ini. Salah satu serangan yang paling mengancam dalam konteks SDN adalah *Distributed Denial of Service* (DDoS), terutama serangan jenis *UDP Flood*.

Serangan *UDP Flood* adalah jenis DDoS yang sangat merusak, di mana penyerang membanjiri jaringan dengan sejumlah besar paket *User Datagram Protocol* (UDP)(Gregorius Hendita Artha Kusuma, 2022). Serangan ini dapat menyebabkan perangkat target mengalami kelebihan beban, yang mengakibatkan gangguan pada layanan, penurunan kinerja jaringan, atau bahkan penghentian total layanan. Di era digital saat ini, ketersediaan dan keamanan jaringan sangat penting bagi institusi bisnis, pemerintahan, dan pendidikan. Berdasarkan laporan dari Cloudflare dan Akamai, terjadi peningkatan lebih dari 50% serangan DDoS pada tahun 2024 dibandingkan dengan tahun sebelumnya(Duncan Riley, 2024). Hal ini menunjukkan bahwa serangan seperti *UDP Flood* semakin meningkat

frekuensinya dan berpotensi menimbulkan kerugian finansial yang signifikan serta mengancam reputasi organisasi yang terdampak.

Untuk mengatasi ancaman tersebut, metode *Rate Limiting* dapat diimplementasikan sebagai langkah mitigasi. *Rate Limiting* adalah teknik yang digunakan untuk membatasi jumlah paket yang diperbolehkan melintasi jaringan dalam jangka waktu tertentu, sehingga dapat mengendalikan arus lalu lintas mencurigakan (admin leravio, n.d.). Dalam konteks SDN, *Rate Limiting* dapat diterapkan menggunakan *Ryu Controller*, yang berfungsi sebagai komponen pengendali SDN. Dengan pengaturan *Rate Limiting*, lalu lintas berlebihan yang mencurigakan seperti paket UDP dalam jumlah besar dapat dikenali dan dibatasi sebelum menyebabkan gangguan serius pada jaringan.

Dalam penelitian ini, tidak hanya dilakukan mitigasi, tetapi juga deteksi serangan menggunakan metode *Machine Learning*, yaitu *Support Vector Machine (SVM)*. Penambahan sistem deteksi ini bertujuan untuk mengidentifikasi lalu lintas abnormal sebelum diteruskan ke tahap mitigasi. *Support Vector Machine (SVM)* merupakan salah satu metode yang baik. Dalam konteks ini, SVM digunakan untuk membedakan antara lalu lintas normal dan lalu lintas serangan *UDP Flood* berdasarkan karakteristik seperti jumlah paket (*Packet Count*) yang dikirim dalam suatu interval waktu. Integrasi deteksi berbasis SVM dan mitigasi berbasis *Rate Limiting* di dalam SDN diharapkan dapat meningkatkan sistem pertahanan secara adaptif (Muhammad Salim Mursid, 2024)

Penelitian ini fokus pada penerapan metode *Rate Limiting* untuk mengatasi serangan DDoS jenis *UDP Flood* dalam arsitektur SDN. Diharapkan bahwa mitigasi ini dapat memberikan solusi untuk meningkatkan keamanan dan ketersediaan jaringan, sehingga dapat melindungi operasional organisasi dari gangguan dan ancaman keamanan siber yang semakin meningkat.

I.2 Perumusan Masalah

Dengan demikian, rumusan masalah yang menjadi dasar penelitian ini adalah sebagai berikut:

1. Bagaimana implementasi serangan *UDP Flood* pada SDN?

2. Bagaimana metode SVM dapat digunakan untuk mendeteksi lalu lintas serangan secara *real-time*?
3. Bagaimana implementasi mitigasi serangan *UDP Flood* dengan metode *Rate Limiting* pada SDN?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Menjalankan metode *Rate Limiting* pada *Ryu Controller* untuk serangan DDoS *UDP Flood* di SDN.
2. Mengintegrasikan metode deteksi berbasis *Machine Learning* (SVM) untuk mendeteksi lalu lintas serangan *UDP Flood*.
3. Mengimplementasikan metode mitigasi serangan *UDP Flood* menggunakan *Rate Limiting* pada SDN melalui *Ryu Controller*, dengan tujuan untuk membatasi laju serangan jaringan.

I.4 Batasan Penelitian

Terdapat beberapa batasan pada penelitian ini, antara lain:

1. Penelitian ini hanya tahap simulasi menggunakan emulator jaringan *Mininet* versi 2.3.1b4 yang berjalan di sistem operasi Ubuntu 20.04.6 LTS dalam lingkungan virtual VMWare Workstation 16 Pro.
2. Solusi ini tidak ada aspek biaya.
3. Skenario serangan yang diuji hanya jenis *UDP Flood* dan tidak mencakup berbagai variasi serangan DDoS lainnya.

I.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Bagi industri dan organisasi: Penelitian ini diharapkan dapat menawarkan solusi yang lebih baik untuk mitigasi serangan DDoS, khususnya untuk organisasi yang menggunakan jaringan berbasis SDN, yang akan meningkatkan keamanan jaringan dan kontinuitas layanan.
2. Bagi akademisi dan peneliti lain: Penelitian ini diharapkan dapat membantu akademisi dan peneliti lain dalam mengembangkan metode mitigasi serangan DDoS berbasis SDN.

3. Bagi pengelola jaringan: Penelitian ini dapat membantu pengelola jaringan menerapkan solusi berbasis SDN untuk mengatasi serangan DDoS dan mempertahankan keandalan dan keamanan jaringan.

I.6 Sistematika Penulisan

Bab I – Pendahuluan

Bab ini menjelaskan latar belakang, perumusan masalah, tujuan, batasan, dan manfaat dari penelitian ini. Tujuannya untuk memberikan gambaran umum dari penelitian ini.

Bab II – Tinjauan Pustaka

Bab ini berisikan kajian teori dan literatur yang relevan dengan topik penelitian, termasuk konsep dasar tentang SDN, DDoS, *UDP Flood*, *Ryu Controller*, *SVM*, *Rate Limiting*.

Bab III – Metodologi Penelitian

Bab ini membahas mulai dari kerangka berpikir, sistematika penyelesaian masalah, pengumpulan data, pengolahan data dan pengembangan sistem, hingga metode evaluasi dan alasan pemilihan metode yang digunakan.

Bab IV – Analisis dan Perancangan

Bab ini menjelaskan tahap perancangan sistem secara teknis, termasuk spesifikasi perangkat keras dan lunak, rancangan topologi SDN di *Mininet*, implementasi *Ryu Controller*, *SVM* dan mitigasi *Rate Limiting*,

Bab V – Hasil dan Analisis

Bab ini menyajikan hasil pengujian dari sistem yang telah dibangun melalui dua skenario utama: kondisi jaringan normal dan saat terjadi serangan *UDP Flood*. Hasil dianalisis menggunakan *confusion matrix* dan log, serta ditampilkan melalui Dashboard visual, di mitigasi menggunakan *Rate Limiting* dan menganalisis kondisi *traffic* normal.

Bab IV – Kesimpulan dan saran

Bab terakhir ini merupakan kesimpulan dari hasil penelitian yang telah dilakukan serta memberikan saran untuk pengembangan sistem di masa mendatang agar lebih optimal dan adaptif terhadap berbagai jenis serangan jaringan lainnya.