BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi telah mendorong transformasi digital di berbagai sektor, mulai dari industri, pemerintahan, hingga layanan publik. Di tengah kemajuan ini, jaringan komputer menjadi infrastruktur utama yang menopang konektivitas, komunikasi, dan pertukaran data secara *real-time.* Untuk menjawab kebutuhan jaringan yang fleksibel, efisien, dan mudah dikonfigurasi, muncul pendekatan baru bernama *Software Defined Networking* (SDN). SDN menawarkan arsitektur jaringan yang memisahkan fungsi pengendalian *(control plane)* dan pengalihan data *(data plane)*, sehingga pengelolaan jaringan dapat dilakukan hanya melalui *controller* (Fitrian et al., 2025).

Penerapan SDN mengalami pertumbuhan pesat seiring meningkatnya kebutuhan akan jaringan yang efisien dan mudah konfigurasi secara terpusat (Puteri Ananda Khairunnisa et al., 2024). Berdasarkan laporan dari *Grand View Research*, nilai pasar SDN secara global diperkirakan mencapai USD 34,29 miliar pada tahun 2023, dan diproyeksikan meningkat hingga USD 101,33 miliar pada tahun 2030, dengan CAGR sekitar 17,9% pada periode 2024–2030. Laporan ini menegaskan bahwa SDN akan terus memegang peran sentral dalam pengembangan infrastruktur jaringan di masa mendatang (Grand View Research, 2023).

Namun, meskipun memiliki banyak keunggulan, SDN yang bersifat terpusat masih memiliki kelemahan, terutama dalam hal keamanan karena semua kendali jaringan berada di controller. Salah satu ancaman serius yang dapat mengganggu kestabilan jaringan adalah *Distributed Denial of Service* (DDoS). Dalam SDN, serangan DDoS dapat membanjiri *controller* dengan lalu lintas palsu sehingga *controller* tidak bisa memproses permintaan yang sah dari pengguna.

Serangan DDoS merupakan salah satu ancaman keamanan siber yang terus meningkat dalam beberapa tahun terakhir. Berdasarkan laporan dari Cloudflare, pada tahun 2023 tercatat lebih dari 8,7 juta serangan yang menargetkan lapisan jaringan secara global (Cloudflare, 2024). Jumlah ini terus bertambah di tahun berikutnya. Pada tahun 2024, Cloudflare berhasil memitigasi lebih dari 21 juta

serangan DDoS, dengan ratusan di antaranya tergolong sebagai serangan berskala besar dengan intensitas melebihi 1 terabit per detik (Cloudflare, 2025).

Salah satu jenis serangan DDoS yang umum digunakan adalah *DNS Amplification Attack.* Serangan ini memanfaatkan kelemahan *server* DNS terbuka. Penyerang mengirim permintaan DNS palsu dengan alamat IP korban, sehingga *server* DNS akan mengirim respons berukuran besar ke korban dengan ukuran respons jauh lebih besar dari permintaan, hal ini menyebabkan *controller* dapat terbebani. Jika serangan ini terjadi maka *controller* akan terbebani dan menyebabkan seluruh sistem jaringan terganggu (Ginting et al., 2023).

Untuk mengurangi dampak dari serangan *DNS Amplification*, salah satu metode mitigasi yang dapat digunakan adalah *rate limiting*. Teknik ini bekerja dengan membatasi jumlah permintaan atau respons, sehingga lalu lintas mencurigakan yang datang secara berlebihan dapat dibatasi atau diblokir sejak awal tanpa mengganggu lalu lintas normal dari pengguna yang sah (Haniyah et al., 2024).

Meskipun *rate limiting* telah banyak digunakan pada jaringan tradisional dan terbukti membantu mengurangi serangan, penerapannya dalam arsitektur SDN yang memiliki karakteristik berbeda masih belum banyak diteliti. Masih terdapat keterbatasan pengetahuan tentang sejauh mana *rate limiting* dapat menjaga kestabilan dan kinerja SDN saat menghadapi serangan *DNS Amplification*. Oleh karena itu, penelitian ini bertujuan untuk menerapkan dan menguji teknik *rate limiting* sebagai strategi mitigasi dalam menghadapi serangan tersebut di lingkungan SDN. Melalui pengujian ini, diharapkan dapat diperoleh pemahaman yang lebih baik tentang ketahanan SDN, serta memberikan kontribusi dalam pengembangan solusi keamanan yang lebih responsif di masa depan.

I.2 Perumusan Masalah

Beberapa masalah yang perlu di perhatikan dalam penelitian ini adalah:

1. Bagaimana implementasi serangan DNS *Amplification* pada SDN?
2. Bagaimana mitigasi terhadap serangan DNS *Amplification* dapat diterapkan pada SDN dengan memanfaatkan *rate limiting?*

3. Bagaimana hasil perbandingan performa jaringan sebelum dan sesudah diterapkan mitigasi *rate limiting* terhadap serangan *DNS Amplification*?

I.3 Tujuan Penelitian

Tujuan perancangan penelitian ini adalah untuk memberikan solusi yang terukur dalam meningkatkan keamanan serta kinerja SDN dalam menghadapi ancaman serangan *DNS Amplification*. Berikut adalah tujuan penelitian berdasarkan permasalahan yang telah diidentifikasi:

1. Mengidentifikasi serangan DNS *Amplification* serta memahami implementasi serangan tersebut pada SDN.
2. Menganalisis penerapan *rate limiting* dalam mengurangi dampak serangan *DNS Amplification* pada SDN.
3. Mengevaluasi strategi mitigasi terhadap performa jaringan dalam menghadapi serangan *DNS Amplification* pada SDN.

I.4 Batasan Penelitian

Penelitian ini difokuskan pada analisis dampak serangan *DNS Amplification* terhadap kinerja jaringan dalam SDN serta penerapan strategi mitigasi menggunakan *rate limiting*. Batasan-batasan yang menjadi fokus dalam penelitian ini sebagai berikut:

1. Fokus penelitian ini hanya pada serangan *DNS Amplification* dan tidak mencakup jenis serangan DDoS lainnya.
2. Pengujian mitigasi dilakukan menggunakan Mininet sebagai emulator jaringan.
3. Implementasi mitigasi dalam penelitian ini terbatas pada penggunaan metode *rate limiting*.
4. Penelitian ini hanya mencakup pengujian mitigasi pada level jaringan dan tidak membahas mitigasi pada level aplikasi atau sistem lainnya.
5. Data lalu lintas yang digunakan dalam pengujian merupakan data simulasi dan bukan berasal dari lalu lintas nyata.

I.5 Manfaat Penelitian

Penelitian ini memiliki tujuan utama untuk memberikan solusi terhadap permasalahan keamanan pada SDN, khususnya dalam mitigasi serangan DNS *Amplification* melalui penerapan mitigasi *rate limiting*. Dengan solusi ini, penelitian ini diharapkan dapat memberikan kontribusi positif yang tidak hanya bermanfaat dalam aspek teknis, tetapi juga berdampak pada berbagai pemangku kepentingan, seperti praktisi, industri, dan masyarakat luas.

Manfaat penelitian ini dijabarkan sebagai berikut:

1. Bagi Praktisi, Penelitian ini menawarkan cara baru untuk menangani serangan *DNS Amplification* pada SDN. Hasil penelitian ini bisa digunakan oleh praktisi untuk membuat solusi keamanan yang lebih cepat dan efisien. Dengan begitu, mereka dapat mengurangi gangguan pada jaringan dan meminimalkan kerugian yang diakibatkan oleh serangan.
2. Bagi Industri, Penelitian ini memberikan peluang bagi perusahaan teknologi untuk menciptakan produk dan layanan SDN yang lebih aman. Metode mitigasi yang dihasilkan dapat membantu industri bersaing di pasar dengan menyediakan solusi keamanan yang lebih baik dan sesuai dengan kebutuhan pengguna.
3. Bagi Masyarakat, Penelitian ini membantu menciptakan jaringan yang lebih aman, sehingga masyarakat bisa menggunakan layanan digital, seperti aplikasi, *e-commerce*, dan layanan keuangan, dengan lebih nyaman dan aman.
4. Bagi pengembang, penelitian ini dapat menjadi referensi dalam merancang modul mitigasi yang terintegrasi dengan *controller* SDN seperti Ryu.