BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi pada beberapa dekade terakhir membawa perubahan besar dalam dunia jaringan komunikasi. Perkembangan yang menonjol adalah penggunaan *Software Defined Network* (SDN), yang memberikan fleksibilitas dan kontrol yang besar terhadap infrastruktur jaringan [1]. Seiring dengan kemajuan tersebut, banyak organisasi yang mengadopsi teknologi SDN untuk mempercepat pengelolaan jaringan dan meningkatkan efisiensi. Namun, dengan meningkatkan penggunaan teknologi SDN tantangan keamanan yang signifikan juga muncul.

Penggunaan SDN menemui berbagai kendala terutama terkait serangan *Denial of Service* (DoS) yang dapat meng operasional jaringan virtual. Misalnya, menerapkan SDN menggunakan pengontrol *Floodlight* telah menjadi pilihan populer, namun kurangnya keamanan terhadap serangan DOS tetap menjadi kekhawatiran utama [2]. Serangan ini dapat menyebabkan gangguan layanan, penurunan kinerja, dan bahkan kerugian finansial.

Untuk mengatasi tantangan ini, *Intrusion Detection System* (IDS) berbasis *Snort* telah muncul sebagai solusi yang menjanjikan. *Snort* adalah sistem deteksi intrusi *open source* yang telah terbukti efektif dalam mendeteksi dan mencegah berbagai jenis serangan. Dalam konteks jaringan virtual dengan SDN, penerapan *Snort* dapat memberikan lapisan keamanan tambahan untuk mendeteksi serangan DoS dengan cepat dan akurat [3].

Selain itu tren teknologi yang terkait dengan topik ini mencakup pengembangan teknologi alternatif untuk meningkatkan keamanan SDN [4]. Beberapa pendekatan baru termasuk mengintegrasikan kecerdasan buatan *Artificial Intelligence* (AI) dan pembelajaran mesin ke dalam IDS untuk mengidentifikasi pola serangan yang lebih kompleks dan tidak dapat diprediksi. Prinsip metode ini adalah untuk meningkatkan kemampuan mendeteksi dan merespons secara otomatis terhadap ancaman yang berkembang [5].

Dengan menggabungkan IDS *Snort* di lingkungan SDN dengan pengontrol *Floodlight*, tugas akhir ini bertujuan untuk memberikan solusi yang andal terhadap serangan DoS [6]. Prediksi yang muncul adalah integrasi ini dapat mengatasi masalah keamanan yang dihadapi implementasi SDN saat ini. Rencana penggunaan teknologi ini mencakup langkah – langkah implementasi *Snort* pada lapisan keamanan SDN dan menganalisis efektivitasnya dalam mendeteksi serangan DoS [7].

Namun, kendala yang mungkin terjadi mencakup kompleksitas konfigurasi, kemampuan beradaptasi terhadap arsitektur jaringan yang ada, dan kemampuan untuk meningkatkan skala deteksi untuk menghadapi serangan yang semakin canggih [8]. Kesulitan – kesulitan ini harus diatasi melalui pendekatan yang cermat dan pemilihan pengaturan yang sesuai dalam konfigurasi *Snort* [9]. Manfaat yang diharapkan adalah peningkatan keamanan jaringan virtual, pengurangan dampak serangan DoS, dan peningkatan infrastruktur SDN [10].

Mempertimbangkan aspek – aspek tersebut, maka kesimpulan yang dapat diambil adalah bahwa penelitian tugas akhir ini melakukan simulasi untuk menguji kinerja IDS berbasis *Snort* dalam mendeteksi serangan DoS pada jaringan virtual yang dikelola oleh *Floodlight Controller*. Simulasi ini akan mencakup pengaturan lingkungan SDN, konfigurasi IDS *Snort*, serta analisis hasil deteksi serangan DoS. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem keamanan jaringan yang lebih efektif dan responsif terhadap ancaman siber. Oleh karena itu, judul tugas akhir yang diusulkan adalah "**Simulasi IDS berbasis *Snort* untuk mendeteksi serangan DoS pada jaringan virtual menggunakan SDN dengan *Floodlight Controller***". Judul ini mencerminkan fokus penelitian pada integrasi Snort sebagai IDS dengan teknologi SDN dan *Floodlight* untuk meningkatkan deteksi serangan DoS dalam jaringan virtual.

1.2 RUMUSAN MASALAH

Untuk meningkatkan keamanan jaringan virtual menggunakan SDN dengan *Floodlight Controller*, tugas akhir ini mencakup beberapa permasalahan sebagai berikut:

1 Apa masalah keamanan yang muncul pada saat menggunakan SDN dengan *Controller Floodlight* menghadapi serangan DoS?
2 Dengan bantuan SDN *Floodlight*, bagaimana penerapan IDS berbasis *Snort* dapat membantu mendeteksi serangan DoS pada jaringan virtual?
3 Bagaimana sistem IDS berbasis Snort menangani kasus *true positives* dan *true negatives* dalam deteksi serangan DoS?

1.3 BATASAN MASALAH

Dalam penelitian ini, beberapa batasan masalah akan diterapkan untuk melengkapi bidang penelitian:

1 Penelitian ini tidak akan membahas serangan apapun selain DoS.
2 Batasan ini hanya berkonsentrasi pada deteksi dan pencegahan serangan DoS, tanpa memeriksa elemen deteksi untuk serangan jenis lain di jaringan virtual berbasis SDN.
3 Penelitian ini akan membatasi simulasi SDN hanya dengan menggunakan *Floodlight Controller* sebagai kontroler utama. Itu tidak akan melihat perbedaan atau perbandingan dengan kontroler SDN lainnya.
4 Batasan ini tidak mencakup ruang lingkup penelitian pada jaringan virtual skala kecil atau menengah, tidak termasuk lingkungan jaringan yang sangat besar atau kompleks.
5 Evaluasi kinerja IDS *Snort* dalam mendeteksi dan mencegah serangan DoS akan fokus pada metrik tertentu seperti waktu respons, akurasi deteksi, dan beban kerja jaringan tanpa memperlihatkan aspek yang lebih luas atau kompleksitas penilaian kinerja.
6 Penelitian ini hanya akan membahas teknologi pendukung untuk menerapkan IDS *Snort* pada *Controller Floodlight* dan SDN. Tidak akan membahas integrasi dengan teknologi keamanan lainnya.

1.4 TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah:

1 Mengevaluasi fitur serangan DoS pada jaringan virtual yang dibangun berdasarkan SDN dengan *Floodlight Controller*.
2 Mengidentifikasi masalah keamanan dan kelemahan yang muncul saat menggunakan SDN dengan *Floodlight Controller* untuk melawan serangan DoS.
3 Mengimplementasikan IDS berbasis *Snort* untuk mendeteksi dan mencegah serangan DoS pada jaringan virtual menggunakan SDN dan pengontrol *Floodlight*.
4 Mengevaluasi kemanjuran dan efisiensi implementasi IDS *Snort* dalam menghadapi serangan DoS pada SDN.

1.5 MANFAAT

Hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1 Memberikan wawasan terhadap kelebihan dan kekurangan keamanan yang diperhatikan saat menerapkan SDN dengan *Floodlight Controller*.
2 Menyediakan solusi praktis untuk mendeteksi dan mencegah serangan DoS pada jaringan virtual pada SDN melalui penerapan IDS) berbasis Snort.
3 Mengambil bagian dalam pengembangan keamanan jaringan virtual dan teknologi SDN secara keseluruhan.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan penelitian ini dibagi menjadi 3 bagian:

1 BAB I : PENDAHULUAN

   Bagian pendahuluan berisi mengenai latar belakang, rumusan masalah yang diangkat, manfaat dan tujuan penelitian.
2 BAB II : DASAR TEORI

   Pada bagian ini membahas tentang referensi penelitian sebelumnya, landasan teori mengenai IDS, *Snort*, SDN, *Floodlight Controller*.
3 BAB III : METODE PENELITIAN

Pada bagian ini membahas mengenai alat dan bahan yang digunakan, rancangan topologi, implementasi sistem, penjelasan pada tiap masing – masing perintah, dan pengujian sistem

4 BAB IV : HASIL DATA DAN PEMBAHASAN

Bagian ini membahas mengenai hasil data berupa hasil perancangan sistem dan hasil pengujian sistem terhadap IDS *Snort* dalam mendeteksi serangan DoS dengan menggunakan SDN *Floodlight.*

5 BAB V : PENUTUP

Bagian ini memberikan kesimpulan dan saran pada hasil penelitian yang berkaitan dengan masalah dalam penelitian.