BAB I PENDAHULUAN

I.1 Latar Belakang

Software Defined Network (SDN) telah menjadi pendekatan yang semakin populer dalam manajemen jaringan. SDN memungkinkan pengelolaan dan implementasi jaringan yang lebih fleksibel, dinamis, dan terpusat, untuk mendukung kebutuhan di bidang ini, tetapi juga membawa risiko baru terkait keamanan.

Terdapat banyak serangan yang mungkin terjadi pada SDN seperti, Manipulasi Jaringan, Pengalihan Lalu Lintas, Manipulasi Aplikasi, *Denial of Service* (DoS), *ARP Spoofing*, Eksploitasi API, Pemantauan Lalu Lintas, dan penebakan kata sandi. Serangan yang difokuskan pada penelitian ini adalah *Distributed Denial-of-Service* (DDoS). DDoS adalah bentuk perluasan dari serangan DoS. DoS adalah serangan *cyber* di mana tujuannya adalah membuat mesin tidak tersedia bagi pengguna dengan mengganggu layanan host dan dilakukan dengan membanjiri target dengan permintaan dan membebani sistem. Pada *Distributed DoS* (DDoS), permintaan tersebut dikirim dari banyak sumber yang membuat sulit untuk menghentikan serangan, berbeda dengan saat hanya satu sumber menyerang karena satu sumber dapat diblokir tetapi banyak sumber sulit diidentifikasi.

Serangan *Distributed Denial of Service* (DDoS) merupakan salah satu ancaman utama dalam dunia siber. Serangan ini bertujuan untuk mengganggu layanan jaringan dengan cara menghambat akses pengguna yang dapat menyebabkan kerugian finansial dan reputasi. Serangan DDoS saat ini semakin canggih dan sulit dideteksi karena memiliki bentuk, intensitas, ataupun sumber yang bervariasi. Dengan serangan yang terus berkembang, maka mengharuskan penggunaan solusi deteksi yang lebih tidak kalah cerdas.

Serangan Denial of Service (DoS) seringkali merupakan kegiatan awal dalam karir seorang hacker. Alasan-alasan politik dan ekonomi saat ini juga menjadi yang paling relevan. Dalam konteks perang cyber, serangan DoS bahkan terjadi secara terdistribusi yang dikenal dengan istilah 'Distributed Denial of Service' (DDoS). Contoh-contoh kasus serangan virus seperti 'code-red' bahkan dapat secara otomatis melancarkan serangan DoS dengan memanfaatkan komputer yang terinfeksi. Lebih penting lagi, motif keisengan seringkali menjadi pendorong utama. Mendapatkan program-program DoS *seperti nestea, teardrop, land, boink, jolt,* dan *vadim* tidaklah sulit. Program-program DoS ini dapat dengan tepat melancarkan serangan Denial of Service, dan yang lebih krusial, sangat mudah untuk dilakukan (Gon, 2012).

Serangan ini menjadi pilihan yang menarik karena ini merupakan serangan yang menghancurkan dan penelitian terhadap serangan ini masih terus dilakukan. Oleh karena itu, penulis berusaha untuk menerapkan teknik *Deep Learning* dalam menghadapi serangan DDOS. Walaupun teknik *Machine Learning* telah banyak diterapkan diluar sana, namun teknik *Deep Learning* lebih efisien dan secara otomatis mendeteksi fitur-fitur yang dapat digunakan untuk mendeteksi serangan tersebut.

Deep Learning menawarkan kemampuan untuk memproses dan memahami data yang kompleks, termasuk data lalu lintas jaringan. Keunggulan *Deep Learning* adalah kemampuannya dalam memperoleh pola yang kompleks dari suatu data. Keunggulan SDN dalam Implementasi: Jaringan SDN yang memungkinkan visibilitas lebih besar terhadap lalu lintas jaringan, dapat digunakan untuk analisis dan deteksi serangan DDoS. Sehingga menghasilkan potensi untuk menggabungkan teknologi SDN dengan Deep Learning untuk mendeteksi serangan yang lebih akurat dan cepat.

I.2 Perumusan Masalah

Berdasarkan analisis latar belakang, terdapat beberapa rumusan permasalahan dari penelitian adalah sebagai berikut.

1. Bagaimana mengukur dan meningkatkan efektivitas sistem deteksi serangan DDoS pada SDN dengan *Deep Learning* dalam mengidentifikasi serangan dan meminimalisir kesalahan?

2. Bagaimana kinerja *Deep Learning* dalam melakukan klasifikasi serangan DDoS?

I.3 Tujuan Tugas Akhir

Tujuan permasalahan dari penelitian adalah sebagai berikut.

1. Sistem deteksi serangan DDoS yang efektif berbasis *Deep Learning* pada lingkungan *Software Defined Network* (SDN).

2. Keamanan jaringan SDN dengan mengidentifikasi serangan DDoS secara akurat dan memberikan respon yang cepat.

I.4 Batasan Tugas Akhir

Batasan tugas akhir ini adalah sebagai berikut:

1. Pengujian dilakukan pada Virtual Machine dan menggunakan Ubuntu versi 20.04
2. Simulasi serangan DDoS menggunakan Hping3.
3. Kemampuan model pada kondisi jaringan yang berbeda.

I.5 Manfaat Tugas Akhir

Manfaat dari penelitian yang dilakukan adalah sebagai berikut:

1. Penelitian ini bermanfaat dalam memberi kontribusi untuk meningkatkan keamanan jaringan SDN dengan mengembangkan sistem deteksi serangan DDoS.

2. Penelitian ini memperlihatkan potensi *Deep Learning* sebagai salah

satu metode deteksi serangan DDoS yang mendukung operasional pada jaringan SDN.

3. Kesuksesan penelitian ini diharapkan dapat memberikan kontribusi dalam menghadapi ancaman serangan DDoS.

I.6 Sistematika Penulisan

Tugas akhir ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Pada bab ini berisi uraian mengenai konteks permasalahan, latar belakang permasalahan, perumusan masalah yang bertujuan untuk menyelesaikan masalah dengan menciptakan sistem terintegrasi yang terdiri dari manusia dengan material dan/atau peralatan/mesin dan/atau informasi dan/atau energy, batasan tugas akhir, manfaat tugas akhir, dan sistematika penulisan.

Bab II Tinjauan Pustaka

Bab ini berisi literatur yang relevan dengan permasalahan yang diambil dan dibahas pula hasil-hasil referensi buku/ penelitian/ referensi lainnya yang dapat digunakan untuk merancang dan menyelesaikan masalah. Minimal terdapat lebih dari satu metodologi/metode/kerangka kerja yang disertakan pada bab ini untuk menyelesaikan permasalahan atau meminimalisir gap antara kondisi eksisting dengan target. Pada akhir bab ini, analisis pemilihan metodologi/metode/kerangka kerja harus dijelaskan untuk menentukan metodologi/metode/kerangka kerja yang

akan digunakan di tugas akhir ini.

Bab III Metodologi Penyelesaian Masalah

Metodologi penyelesaian merupakan penjelasan metode / konsep / kerangka kerja yang telah dipilih pada bab Tinjauan Pustaka. Pada tugas akhir Pada bab ini dijelaskan langkah-langkah tugas akhir secara rinci meliputi: tahap merumuskan masalah, merumuskan hipotesis, mengembangkan model, mengidentifikasi dan melakukan

operasionalisasi variabel, menyusun kuesioner, merancang pengumpulan dan pengolahan data, melakukan uji instrumen, merancang analisis pengolahan data dalam rangka perancangan sistem terintegrasi untuk penyelesaian permasalahan.

Bab IV Perancangan Sistem Terintegrasi

Seluruh kegiatan dalam rangka perancangan sistem terintegrasi untuk penyelesaian masalah dapat ditulis di bab ini. Kegiatan yang dilakukan dapat berupa pengumpulan dan pengolahan data, pengujian data, dan perancangan solusi.

Bab V Analisa Hasil dan Evaluasi

Pada bab ini, disajikan hasil rancangan, temuan, analisis dan pengolahan data. Selain itu bab ini juga berisi tentang validasi atau verifikasi hasil dari solusi, sehingga hasil tersebut apakah telah benar-benar menyelesaikan masalah atau menurunkan gap antara kondisi eksisting dan target yang ingin dicapai. Analisis sensitivitas juga dapat digunakan di bab ini untuk lebih mengetahui hasil tugas akhir dapat diterapkan baik secara khusus di konteks tugas akhir maupun secara umum di konteks serupa (misal perusahaan di sektor serupa). Selain itu metode-metode evaluasi yang lain dapat di terapkan untuk memvalidasi hasil sesuai dengan kebutuhan.

Secara keseluruhan bab ini membahas secara mendetail mengenai hasil dari pengerjaan solusi dan refleksinya terhadap tujuan tugas akhir.Untuk tugas akhir yang berfokus pada merancang sistem informasi/ aplikasi maka penamaan bab ini mengikuti tahapan penerapan SDLC yang digunakan dalam tugas akhir.

Bab VI Kesimpulan dan Saran

Pada bab ini dijelaskan kesimpulan dari penyelesaian masalah yang dilakukan serta jawaban dari rumusan permasalahan yang ada pada bagian pendahuluan. Saran dari solusi dikemukakan pada bab ini untuk tugas akhir selanjutnya.