BAB I PENDAHULUAN

I.1 Latar Belakang

Jaringan pada setiap sektor kehidupan, khususnya pada infrastruktur, sangat berpengaruh satu sama lain. Salah satu jenis jaringan yang sering kita temui dalam kehidupan sehari-hari adalah LAN (Local Area Network). LAN banyak digunakan di berbagai tempat seperti café, kampus, kantor, hingga rumah. Sebagai penghubung antar perangkat di area lokal, LAN mempermudah pertukaran data dan penggunaan sumber daya bersama, misalnya akses internet atau berbagi printer. Meski begitu, pengelolaan jaringan, terutama pada tingkat enterprise, tidaklah mudah. Kompleksitas jaringan pada skala besar memerlukan berbagai alat dan teknik yang canggih untuk memastikan jaringan tetap aman, stabil, dan efisien.

Seiring perkembangan teknologi, kebutuhan akan solusi pengelolaan jaringan yang lebih fleksibel dan dinamis semakin meningkat. Salah satu solusi yang menjawab tantangan ini adalah Software Defined Network (SDN), yang memberikan pendekatan baru dalam manajemen jaringan. Dalam arsitektur SDN, administrator dapat mengontrol lalu lintas jaringan dari pusat, melalui software, baik dari cloud maupun secara remote. SDN memisahkan fungsi pengendalian jaringan dari perangkat keras dan memindahkannya ke pengendalian berbasis software, yang memungkinkan pengelolaan jaringan lebih mudah, cepat, dan terpusat.

Namun, meskipun SDN menawarkan berbagai kemudahan dan efisiensi, teknologi ini tidak kebal terhadap ancaman siber, terutama serangan Distributed Denial of Service (DDoS). DDoS adalah jenis serangan siber di mana penyerang mengirimkan lalu lintas palsu secara terus menerus dengan volume yang sangat besar, bertujuan untuk membuat sistem kewalahan dalam menangani permintaan yang masuk. Akibatnya, sistem menjadi lambat atau bahkan tidak bisa diakses sama sekali, yang dapat menyebabkan kerugian besar bagi organisasi, terutama jika serangan ini menargetkan layanan kritikal.

Menurut laporan dari Cloudflare, pada kuartal ketiga tahun 2023, serangan DDoS mengalami peningkatan sebesar 65% dibandingkan kuartal sebelumnya. Hal ini menunjukkan bahwa serangan DDoS semakin berkembang, baik dari segi

kompleksitas maupun frekuensinya. Bahkan, Cloudflare mencatat bahwa kuartal ketiga tahun 2023 adalah periode dengan serangan DDoS paling rumit dan berat yang pernah dihadapi. Peningkatan ini membuat organisasi di seluruh dunia harus lebih waspada dan mengadopsi langkah-langkah yang lebih efektif untuk melindungi infrastruktur mereka.

Dalam menangani ancaman DDoS, salah satu pendekatan yang dapat digunakan adalah melalui controller di jaringan SDN. Controller SDN berperan sebagai pusat kendali yang memantau dan mengelola lalu lintas jaringan. Oleh karena itu, penting bagi controller untuk dapat bertindak dengan cepat dan efektif dalam menghadapi serangan DDoS. Namun, agar tidak membebani kinerja controller itu sendiri, metode yang digunakan untuk mendeteksi serangan haruslah ringan dan efisien.

Penulis membangun sistem deteksi DDoS pada jaringan SDN menggunakan machine learning dengan algoritma Naïve Bayes sebagai pendekatan untuk mengklasifikasikan serangan. Naïve Bayes dipilih karena algoritma ini dikenal ringan, cepat, dan mampu menangani data dengan volume besar secara efisien. Penggunaan Naïve Bayes diharapkan dapat mendeteksi serangan DDoS dengan akurasi yang baik, sambil tetap menjaga kinerja jaringan agar tidak terpengaruh oleh proses deteksi yang berlangsung. Sistem ini akan memantau lalu lintas jaringan secara real-time, menganalisis pola data, dan memprediksi apakah lalu lintas tersebut merupakan serangan DDoS atau lalu lintas normal.

I.2 Perumusan Masalah

Rumusan Masalah yang mendasari penelitian ini adalah:

a. Bagaimana sistem yang dibuat dapat mendeteksi serangan Distributed Denial of Service (DDoS) pada jaringan *Software Defined Network* (SDN) dengan *machine learing* menggunakan Naïve Bayes?
b. Bagaimana kinerja *machine learing* model algoritma Naïve Bayes dalam melakukan klasifikasi serangan DDoS?

I.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

a. Sistem deteksi serangan DDoS pada jaringan SDN dengan *machine learing* menggunakan Naïve Bayes.
b. Pengujian keakuratan klasifikasi serangan DDoS menggunakan *machine learing* model algoritma Naïve Bayes.

I.4 Batasan Penelitian

Ruang lingkup pembahasn yang digunakan dalam penelitian ini antara lain:

1. Pengujian pada jaringan lokal.
2. Deteksi DDoS secara real time.
3. Menggunakan Ubuntu versi 22.04.4

I.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

1. Mendalami ilmu serta pengetahuan peneliti tentang sistem deteksi serangan DDoS pada sdn dengan *machine learing* menggunakan Naïve Bayes.
2. Bagi peneliti lain yang bergerak dalam bidang keamanan jaringan, penelitian ini bermanfaat untuk mengembangkan penelitian deteksi serangan DDoS pada SDN dengan Naïve Bayes.

I.6 Sistematika Penelitian

Pada penyusunan tugas akhir ini terdiri dari enam bab yang dapat di uraikan sebagai berikut:

1. BAB I PENDAHULUAN

   Pembahasan pada pendahuluan menjelaskan tentang apa yang mendasari dari penelitian ini. Hal tersebut menyangkut latar belakang, perumusuan masalah, tujuan dari penelitian, batasan pada penelitian, manfaat dari penelitian, dan sistematika penulisan dari penelitian yang dilakukan.

2. BAB II LANDASAN TEORI

   Pembahasan pada landasan teori berisikan literatur-literatur dan teori dasar yang relevan dengan penelitian yang dilakukan berdasarkan referensi yang didapatkan.

3. BAB III METODOLOGI PENELITIAN

   Pembahasan pada metodologi penelitian menjelaskan secara rinci mentode yang digunakan dalam penelitian. Ini mencakup data yang dikumpulkan, teknik pengumpulan data, serta perangkat atau tools yang digunakan. Selain itu, metodologi juga mencakup pendekatan analisi yang digunakan untuk mengolah data yang diperoleh.

4. BAB IV ANALISIS DAN PERANCANGAN

   Pembahasan pada analisis dan perancangan berfokus pada analisis data yang telah dikumpulkan selama penelitian. Analisis ini membantu dalam pemahaman yang lebih mendalam tentang penelitian.

5. BAB V IMPLEMENTASI DAN PENGUJIAN

   Pembahasan pada implementasi dan pengujian akan membahas implementasi dari rencana perancangan yang telah dibuat sebelumnya serta hasil yang didapatkan setelahnya.

6. BAB VI KESIMPULAN DAN SARAN

   Pembahasan pada kesimpulan dan saran berisi rangkuman temuan utama dari penelitian. Selain itu, akan diberikan saran-saran berdasarkan hasil penelitian ini, yang dapat digunakan sebagai panduan untuk pengembangan di masa depan.