BAB I

PENDAHULUAN

1. 1. Latar Belakang

Dalam dunia teknologi yang terus berkembang, keamanan siber sangat penting seiring dengan kemajuan pesat dalam digitalisasi, ketergantungan pada teknologi telah meningkat secara eksponensial, membuat pemerintah, lembaga, dan individu sangat bergantung pada sistem yang saling terhubung. Oleh karena itu, potensi ancaman yang ditimbulkan oleh ancaman cyber menjadi lebih jelas dan meluas. Salah satu serangan yang merusak dan meresahkan adalah *Distributed Denial of Service* (DDoS). Serangan DDoS merupakan serangan yang bertujuan untuk membuat layanan tidak tersedia menggunakan berbagai sumber yang terdistribusi (Fauzi et al., 2023).

Bidang keamanan siber terus mengalami perkembangan yang dinamis sebagai akibat dari peningkatan jumlah ancaman dan serangan siber yang canggih yang dihadapi oleh berbagai organisasi. Memastikan bahwa pertahanan keamanan siber yang tangguh dan kemampuan ketahanan yang kuat telah menjadi suatu keharusan yang sangat penting. Untuk menghadapi tantangan-tantangan tersebut, perusahaan-perusahaan telah mengadopsi berbagai metode deteksi. Di antara metode-metode tersebut termasuklah *data mining* yang merupakan salah satu yang bertujuan untuk mendapatkan pengetahuan dari informasi-informasi yang didapatkan sebelumnya.

Pada PT. ABC terjadi serangkaian serangan *Distributed Denial of Service* (DDoS) yang menyebabkan kerugian finansial dan gangguan operasional. Hal ini

terjadi dikarenakan kurangnya solusi deteksi serangan DDoS yang lebih responsif, akurat, dan efektif. Solusi yang diusulkan untuk menangani hal tersebut adalah dengan deteksi serangan menggunakan pendekatan *data mining*, menggunakan teknik *machine learning*.

Deteksi serangan adalah merupakan bidang yang berkembang terus menerus dalam upaya untuk melindungi sistem dan data. Salah cara yang digunakan dalam deteksi adalah dengan menggunakan metode *data mining*. Karena beberapa kasus, algoritma mencapai akurasi yang kurang mumpuni. Penelitian ini bertujuan untuk memberikan kontribusi solusi dalam mendeteksi serangan DDoS. Hasil dari penelitian ini berpotensi untuk memberikan pemahaman penggunaan *machine learning* dalam deteksi serangan DDoS. Penelitian juga dapat memberikan wawasan bagi para *security professional* untuk mengembangkan solusi yang lebih aman dan efektif untuk melindungi sistem komputer dan data sensitif.

1. 2. Rumusan Masalah

Dari latar belakang masalah di atas dapat diuraikan permasalahan sebagai berikut:

1. Bagaimana cara menerapkan algoritma *data mining* untuk Mendeteksi Serangan DDoS ?
2. Bagaimana hasil kinerja matrix confussion dari penerapan algoritma datamining untuk Mendeteksi Serangan DDoS ?

1. 3. Batasan Masalah

1. Data masukan berupa merupakan data serangan yang nantinya dikategorikan menjadi 2 yaitu *DDoS* dan *Benign*.

2. Data yang digunakan merupakan data sekunder dan merupakan data simulasi serangan yang dihasilkan berdasarkan dunia nyata.D
3. *Deployment data mining* akan menggunakan Flask sebagai kerangka kerja untuk membangun aplikasi web yang memungkinkan pengguna untuk melakukan deteksi serangan DDoS.

1. 4. Tujuan dan Manfaat

1. 4. 1. Tujuan

Tujuan dari penelitian ini adalah:

1. Mempelajari dan menganalisis serangan DDoS dengan menggunakan teknik data mining dengan pendekatan machine learning.
2. Mengidentifikasi algoritma machine learning yang paling efektif untuk membangun model mendeteksi serangan DDoS berbasis machine learning.
3. Membangun sistem deteksi serangan DDoS berbasis web dengan menggunakan kerangka kerja flask untuk melakukan deteksi secara real time dan membuat visual hasilnya dengan cepat dan mudah.

1. 4. 2. Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Model prediksi membantu PT. ABC untuk mendeteksi serangan DDoS di masa mendatang.
2. Meningkatkan reputasi PT. ABC yang dapat meningkatkan kepercayaan dan loyalitas pelanggan dengan terbuktinya dapat menghadapi dan mengatasi serangan siber dengan efektif.

3. Membantu PT. ABC dalam memenuhi kepatuhan dan regulasi terkait keamanan siber.
4. Meningkatkan reputasi PT. ABC yang dengan meningkatnya kepercayaan dan loyalitas pelanggan dengan terbuktinya dapat menghadapi dan mengatasi serangan siber dengan efektif.

1. 5. Metode Pengumpulan Data

Metode pengumpulan data dalam penelitian ini adalah :

1. Studi Pustaka dan Literature Review

   Mengumpulkan dan mempelajari literatur yang relevan untuk meningkatkan pengetahuan di bidang data mining.
2. Data publik dan sumber terbuka

   Menggunakan data publik dan sumber terbuka seperti kaggle untuk mengumpulkan informasi mengenai serangan DDoS.
3. Data historis: Data historis yang didapatkan dari hasil penangkapan lalu lintas jaringan melalui aplikasi *wireshark*.

1. 6. Sistematika Penulisan

Dalam penulisan penelitian ini menggunakan sistematika penulisan sebagai berikut :

BAB I – PENDAHULUAN

Bagian ini berisi gambaran umum dari penelitian yang terdiri dari latar belakang serangan DDoS dan model prediksi, rumusan masalah mengenai isu serangan DDoS dan akan kebutuhan model prediksi deteksi serangan DDoS, batasan masalah termasuk labeling yang hanya terbatas pada *benign* dan *ddos*, jenis

data yang digunakan dan membahas metode *deployment* menggunakan Flask, tujuan penelitian, metode penulisan, dan sistematika penulisan.

BAB II – LANDASAN TEORI

Berisi ide dan teori dasar yang mendukung pembahasan dalam penelitian yang dapat diterapkan untuk menyelesaikan masalah yang diangkat, seperti pengertian deteksi serangan, pengertian dan faktor-faktor DDoS, serta tinjauan mengenai algoritma yang digunakan.

BAB III – ANALISA DAN PERANCANGAN DESAIN SISTEM

Membahas perancangan sistem yang akan dibuat dalam penelitian ini dan berisi implementasi sistem yang akan dibuat, di antaranya *pre-processing data* hingga parameter yang digunakan dalam penelitian.

BAB IV – HASIL DAN PEMBAHASAN

Membahas hasil dari perancangan implementasi dan analisis sistem seperti tampilan antar muka, hasil *confussion matrix*, dan hasil evaluasi dalam penelitian.

BAB V – PENUTUP

Merupakan rangkuman serta hasil akhir dari semua informasi yang telah disajikan dalam bagian-bagian sebelumnya. Termasuk rekomendasi algoritma yang yang paling efektif dalam pengembangan model prediksi deteksi serangan DDoS.