BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Serangan siber merupakan segala bentuk kejahatan yang menargetkan sistem informasi, jaringan, infrastruktur, telepon genggam, dan komputer personal. Dalam kehidupan dunia saat ini, ketergantungan terhadap internet tidak dapat dihindari. Bentuk serangan siber antara lain adalah serangan *Distributed Denial-of-Service* (DDoS), serangan *phishing*, pembobolan data, dan lain-lain. Pembobolan data mencuri jutaan data pribadi dari orang-orang di seluruh dunia [1]. Data yang dicuri kemudian dijual kepada pihak-pihak yang akan menggunakannya untuk menyebabkan kerugian finansial dan/atau reputasi. Oleh karena itu, diperlukan adanya upaya untuk mendeteksi dan mencegah terjadinya serangan siber.

Untuk mendeteksi dan mencegah serangan siber, dapat dilakukan dengan berbagai cara yang membutuhkan teknologi canggih, kebijakan yang kokoh, dan kewaspadaan. Pencegahan serangan siber dapat dilakukan dengan menggunakan *firewall*, aplikasi *antivirus* dan *anti-malware* yang selalu diperbarui, memberikan edukasi tentang serangan siber, mengenkripsi data yang sensitif, dan sebagainya. Untuk mendeteksi terjadinya serangan siber, dapat digunakan sistem seperti *Intrusion Detection System* (IDS) dan *Endpoint Detection and Response* (EDR), melakukan pengawasan jaringan secara manual maupun otomatis untuk menemukan aktivitas yang mencurigakan, atau menggunakan pembelajaran mesin dan kecerdasan buatan (AI) untuk menganalisis aktivitas di jaringan.

Pengklasifikasian dan deteksi serangan siber menggunakan pembelajaran mesin bukanlah suatu hal yang baru dilakukan. Terdapat beberapa penulis yang telah terlebih dahulu melakukan penelitian dengan topik serupa, seperti [2] yang menganalisis dan membandingkan beberapa algoritma dalam mengklasifikasikan serangan DDoS dalam lingkungan *network*. P. Elamparithi, dkk. [3] menggunakan algoritma *Random Forest* untuk mendeteksi serangan DDoS pada jaringan *Internet of Things* (IoT). Dalam penelitian ini, akan dibandingkan efektivitas algoritma *Random Forest*, *Logistic Regression*, *Decision Tree*, dan *Support Vector Machines* (SVM) dalam mendeteksi serangan DDoS *Botnet* pada jaringan IoT. Perbandingan keempat algoritma tersebut dilakukan karena algoritma-algoritma ini merupakan metode yang umum digunakan dalam sistem deteksi intrusi (IDS) berbasis

pembelajaran mesin [4] [5] [6].

Menurut laporan dari NETSCOUT, jutaan serangan DDoS tercatat setiap tahunnya [7]. Cloudflare melaporkan bahwa pada kuartal pertama tahun 2024, terjadi peningkatan signifikan pada serangan DDoS berbasis aplikasi maupun jaringan [8]. Hal ini menegaskan posisi DDoS sebagai salah satu serangan paling umum di lanskap ancaman siber [9, 10]. Fokus penelitian dalam skripsi ini diarahkan pada jaringan *Internet of Things* (IoT). Hal ini disebabkan karena IoT telah menjadi salah satu teknologi yang banyak diadopsi di berbagai bidang, mulai dari kesehatan, transportasi, industri manufaktur [3]. Dalam penelitian ini, akan digunakan *dataset* bernama *Bot-IoT Dataset* dari pembuatan laboratorium UNSW Canberra.

1.2 Rumusan Masalah

1. Bagaimana cara implementasi algoritma *Random Forest*, *Logistic Regression*, *Decision Tree*, dan SVM dalam mendeteksi serangan DDoS dalam jaringan IoT?

2. Manakah dari algoritma *Random Forest*, *Logistic Regression*, *Decision Tree*, dan SVM yang lebih akurat dalam mendeteksi serangan DDoS dalam jaringan IoT dengan cara menghitung dan membandingkan akurasi, presisi, *recall*, dan F1 dari masing-masing algoritma?

1.3 Batasan Permasalahan

1. Serangan DDoS menggunakan metode *Botnet* dalam Jaringan IoT.

2. *Dataset* didapat dari pembuatan laboratorium UNSW Canberra dengan nama "*Bot-IoT Dataset*" [11] [12] [13] [14] [15].

1.4 Tujuan Penelitian

1. Mengimplementasikan algoritma *Random Forest*, *Logistic Regression*, *Decision Tree*, dan SVM dalam mendeteksi serangan DDoS dalam jaringan IoT.

2. Mengetahui manakah dari algoritma *Random Forest*, *Logistic Regression*, *Decision Tree*, dan SVM yang lebih akurat dalam mendeteksi serangan DDoS

dalam jaringan IoT dengan cara menghitung dan membandingkan akurasi, presisi, *recall*, dan F1 dari masing-masing algoritma.

1.5 Manfaat Penelitian

1. Mengetahui bagaimana cara implementasi algoritma *Random Forest*, *Logistic Regression*, *Decision Tree*, dan SVM dalam mendeteksi serangan DDoS dalam jaringan IoT.
2. Mengetahui manakah dari algoritma *Random Forest*, *Logistic Regression*, *Decision Tree*, dan SVM yang lebih akurat dalam mendeteksi serangan DDoS dalam jaringan IoT dengan cara menghitung dan membandingkan akurasi, presisi, *recall*, dan F1 dari masing-masing algoritma.

1.6 Sistematika Penulisan

Berisikan uraian singkat mengenai struktur isi penulisan laporan penelitian, dimulai dari Pendahuluan hingga Simpulan dan Saran.

Sistematika penulisan laporan adalah sebagai berikut:

- Bab 1 PENDAHULUAN
  Bab ini terdiri dari enam bagian, yaitu latar belakang masalah, rumusan masalah, batasan permasalahan, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.
- Bab 2 LANDASAN TEORI
  Bab ini berisi penjelasan mengenai teori, konsep dasar, dan arsitektur dari algoritma yang akan diterapkan pada penelitian ini untuk mendukung proses perancangan sistem dan implementasi algoritma.
- Bab 3 METODOLOGI PENELITIAN
  Bab ini berisi penjelasan mengenai tahapan-tahapan dan alur kerja yang akan dilakukan dalam penelitian.
- Bab 4 HASIL DAN DISKUSI
  Bab ini berisi penjelasan mengenai hasil yang didapatkan melalui penelitian dan diskusi terhadap hasil tersebut.

- Bab 5 KESIMPULAN DAN SARAN
  Bab ini berisi kesimpulan yang diambil dari penelitian yang sudah dilakukan dan saran yang dapat dilakukan oleh penelitian berikutnya.