BAB I
PENDAHULUAN

1.1 Latar Belakang

Serangan *Distributed Denial of Service* (*DDoS*) merupakan salah satu ancaman siber paling serius yang dapat mengganggu ketersediaan layanan jaringan dengan membanjiri lalu lintas data ke suatu sistem target. Serangan ini dapat menyebabkan gangguan operasional, kerugian finansial, serta menurunkan kepercayaan pengguna terhadap layanan digital. *DDoS* sering kali dimanfaatkan oleh aktor jahat untuk menyerang server, layanan *cloud*, maupun infrastruktur jaringan dengan mengarahkan sejumlah besar permintaan yang melebihi kapasitas normal sistem, menyebabkan layanan menjadi lambat atau bahkan tidak dapat diakses sama sekali. Seiring dengan perkembangan teknologi, serangan *DDoS* menjadi semakin kompleks dan sulit dideteksi, karena pelaku serangan kini menggunakan teknik canggih seperti *spoofing IP*, *botnet*, dan serangan berbasis aplikasi untuk menghindari deteksi oleh sistem keamanan tradisional (Sanmorino et al., 2024).

Seiring berkembangnya infrastruktur jaringan dan meningkatnya jumlah perangkat yang saling terkoneksi terutama pada era *Internet of Things* (IoT) maka teknik serangan *DDoS* juga semakin kompleks dan sulit dikenali. Pendekatan konvensional seperti sistem berbasis tanda tangan (*signature-based*) atau deteksi berbasis ambang batas kini mulai kehilangan efektivitas, karena tidak mampu beradaptasi secara dinamis terhadap variasi pola serangan yang baru. Untuk mengatasi keterbatasan tersebut, diperlukan metode yang lebih adaptif dan cerdas. *Machine Learning* (*ML*) hadir sebagai solusi modern yang dapat mempelajari pola perilaku jaringan secara otomatis dan mengenali anomali dalam lalu lintas data dengan tingkat akurasi yang tinggi.

Dalam penelitian ini, digunakan algoritma *Random Forest*, yang merupakan salah satu metode *ML* berbasis ensemble learning yang efektif dalam melakukan klasifikasi data dengan dimensi besar dan struktur tidak seimbang. Algoritma ini memiliki keunggulan dalam mengolah berbagai jenis fitur serta mampu menangani klasifikasi multikelas secara andal. Fokus penelitian diarahkan pada

deteksi serangan *DDoS* karena jenis serangan ini memiliki dampak luas dan sering kali luput dari sistem deteksi tradisional. Dataset CICIDS-2017 dipilih sebagai basis data karena berisi rekaman lalu lintas jaringan yang realistis, lengkap dengan berbagai jenis serangan dan lalu lintas normal, sehingga cocok untuk mengevaluasi performa model deteksi intrusi berbasis machine learning secara komprehensif. (Arief et al., 2017).

Serangan *DDoS* bekerja dengan memanfaatkan botnet (jaringan perangkat terkompromi) untuk mengirim permintaan palsu dalam skala besar ke server target (Haeruddin et al., 2025). Hal ini menyebabkan overload pada kapasitas *bandwidth*, *CPU*, atau memori, sehingga layanan menjadi tidak tersedia bagi pengguna sah. Tantangan utama dalam deteksi *DDoS* adalah membedakan lalu lintas serangan dari lalu lintas normal, terutama karena serangan modern semakin canggih dalam menyamar sebagai traffic yang valid (Laiq et al., 2023)Metode tradisional seperti threshold-based filtering atau signature detection seringkali kurang efektif karena tidak mampu beradaptasi dengan pola serangan yang dinamis. Oleh karena itu, pendekatan berbasis *machine learning* (*ML*) menjadi solusi yang menjanjikan. *ML* mampu menganalisis pola lalu lintas jaringan secara *real-time*, mempelajari karakteristik anomali, dan mengklasifikasikan serangan dengan akurasi tinggi. Beberapa algoritma *ML* telah diuji untuk deteksi *DDoS*, namun belum ada konsensus mengenai model mana yang paling optimal.

Menurut beberapa penelitian, serangan *DDoS* merupakan salah satu jenis serangan siber paling umum dan merugikan, karena mampu menyebabkan downtime, kerugian finansial, dan menurunnya reputasi layanan yang diserang (He et al., 2024). Penggunaan algoritma Random Forest dalam mendeteksi serangan *DDoS* menunjukkan hasil yang menjanjikan dalam berbagai penelitian, dengan tingkat deteksi yang tinggi dan *false positive* yang rendah (Jairu & Mailewa, 2022). Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi kinerja algoritma *Random Forest* dalam mengidentifikasi serangan *DDoS* di lingkungan jaringan.

1.2 Rumusan Masalah

Beberapa permasalahan yang akan dibahas dalam penelitian ini antara lain :

1. Bagaimana performa algoritma *Random Forest* dalam mengklasifikasikan berbagai jenis serangan jaringan berdasarkan dataset CIC-IDS2017?
2. Seberapa efektif *Random Forest* dalam mendeteksi lalu lintas jaringan yang bersifat normal dan anomali dengan tingkat akurasi tinggi?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk :

1. Menganalisis kinerja algoritma *Random Forest* dalam mendeteksi dan mengklasifikasikan jenis-jenis serangan jaringan pada dataset CIC-IDS2017.
2. Mengevaluasi efektivitas model *Random Forest* dalam membedakan lalu lintas jaringan normal dan berbahaya dengan menggunakan metrik akurasi, *precision*, *recall*, dan *confusion matrix*

1.4 Manfaat

Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem deteksi intrusi jaringan berbasis machine learning, khususnya dengan memanfaatkan algoritma *Random Forest* untuk mengklasifikasikan serangan *DDoS* secara otomatis. Dengan akurasi tinggi yang dicapai, model yang dibangun berpotensi diterapkan dalam lingkungan nyata guna membantu administrator jaringan mendeteksi ancaman lebih awal, sehingga sistem dapat lebih terlindungi dari gangguan yang dapat mengakibatkan kerugian operasional maupun keamanan data.