BAB I
PENDAHULUAN

1.1 Latar Belakang

Laporan *We Are Social* melaporkan bahwa pada Januari 2023, sekitar 213 juta orang di Indonesia menggunakan internet, atau 77% dari total populasi 276,4 juta orang. Peningkatan sekitar 5,44% dari angka 202 juta orang pada Januari 2022. Peningkatan yang signifikan ini menunjukkan tren positif masyarakat dalam adopsi teknologi digital. Perkembangan ini berdampak besar pada kehidupan sehari-hari orang dan menunjukkan peran internet yang semakin penting dalam kemajuan sosial dan ekonomi pada negara [1]. Namun, perlu diingat bahwa semakin berkembangnya koneksi internet juga menimbulkan masalah keamanan. Serangan DDoS, juga dikenal sebagai *Distributed Denial of Service*, adalah salah satu ancaman yang muncul. Oleh karena itu, penting untuk terus meningkatkan keamanan internet untuk melindungi infrastruktur digital dari serangan DDoS [2].

Penyerangan *Distributed Denial of Services* atau bisa disebut juga DDOS adalah serangan yang berfokus pada keamanan jaringan computer. Cara kerja serangan ini dengan mengirimkan permintaan dalam jumlah yang besar ke satu *server* yang dikendalikan oleh satu computer dari jarak yang jauh. Akibat dari serangan ini membuat *server* tidak dapat memproses layanan pengguna karena terjadi kelebihan kapasitas dari *server* tersebut sehingga pengguna sah tidak dapat mengakses atau mengirim permintaan kepada *server* [3].

Serangan dari DDOS ini tidak memilih target bisa saja individu, organisasi, bahkan industri. Tujuan dari penyerangan DDOS untuk menolak pengguna yang sah sehingga menghambat *server* untuk memberikan layanan kepada pengguna [4]. Sehingga salah satu pendekatan yang dapat dicegah dalam serangan DDoS adalah dengan mengimplementasikan sistem

deteksi menggunakan *Machine Learning*, dengan menggunakan *Machine Learning* untuk mendeteksi, organisasi dapat melawan serangan DDoS dengan lebih proaktif.

Machine Learning adalah cabang dari ilmu kecerdasan buatan, yang dikhususkan untuk mempelajari bagaimana *computer* mampu belajar dari data yang diberikan hingga akhirnya kecerdasan tersebut dapat memprediksi seusai dengan yang diharapkan [5]. Pada penelitian ini menguji seberapa baik *Machine Learning* yang akan digunakan dalam melakukan pendeteksian antara lain menggunakan model KNN (*K-Nearest Network*) dan *Random Forrest*. Alasan menggunakan model tersebut dikarenakan dalam jurnal yang telah dibaca model tersebut memiliki akurasi yang tinggi dibandingkan dengan model *Machine Learning* lainnya sehingga dengan begitu diharapkan dapat memberikan pilihan yang tepat dalam mendeteksi serangan DDoS.

Menurut penelitian [6] Metode *K-Neurest Network* atau disingkat KNN adalah metode yang cocok untuk mengklasifikasikan serangan DDoS dikarenakan hasil dari penelitian ini memberikan *accuracy* 1 dan pengujian *f1-score*. Dasar dari struktur Pembangunan model ini adalah memberikan parameter nilai K dan pengukuran jarak atau *metric* dengan *Euclidean*. Metode KNN memiliki keunggulan antara lain pelatihan yang sederhana, cepat, mudah dimengerti, dan efektif untuk mengukur data latih yang besar [7].

Menurut penelitian [3], model *Machine Learning* yang digunakan dalam penelitian untuk mendeteksi sebuah data DDOS berupa serangan atau normal. Dengan melatih beberapa model *Machine Learning* terdapat sebuah akurasi yang lebih optimal yaitu *random forest*. Parameter yang biasa dilakukan dalam Pembangunan model adalah *n_estimator*, *max_depth*, *max_features*, dan *bootstraps*. Model ini memiliki kelebihan ketika pelatihan model kemungkinannya kecil terkena overfitting dan kemampuan menanggani data yang tidak seimbang [8].

Dengan melihat perbandingan dari 2 *Machine Learning* bisa dilihat bahwa memiliki kekurangan dan kelebihan masing-masing. Pada *Machine*

Learning memiliki keunggulan Pembangunan model yang tidak terlalu rumit sehingga pelatihan model dapat berlangsung cepat.

Atas dasar tersebut, maka menggunakan beberapa model *Machine Learning* untuk mendeteksi serangan DDoS, model Machine Learning yang di uji untuk penelitian ini yaitu KNN dan *Random Forest*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas dapat diketahui permasalahan dalam penelitian ini adalah bagaimana pengolahan *dataset* agar sesuai dengan masing-masing *Machine Learning*. Serta performa model *Machine Learning* yang telah dipilih dapat memiliki tingkat akurasi yang baik sehingga dapat di terapkan pada pendeteksian serangan DDoS.

1.3 Pertanyaan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan, maka pertanyaan peneliti dalam melakukan penelitian ini adalah:

1. Bagaimana menerapkan klasifikasi *dataset* berformat CSV agar bisa digunakan oleh *Random Forest* dan KNN?
2. Berapa nilai akurasi yang didapatkan oleh masing-masing model *Machine Learning* yang telah dipilih menggunakan *Accuracy*, *F1-Score*, *recall*, dan *precision*?

1.4 Batasan Masalah

Batasan masalah dari penilitian ini adalah :

1. Model *Machine Learning* yang digunakan hanya KNN (*K-Nearest Neighbor*) dan *Random Forest.*
2. Data yang digunakan adalah *Dataset* CICDDoS2019
3. Evaluasi model menggunakan *confussion matrix*

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah dan pertanyaaan penelitian yang sudah dijelaskan, tujuan dari penelitian ini:

1. Menerapkan klasifikasi serangan DDOS dengan *Random Forest* dan KNN

2. Mengukur performa *Accuracy*, *Recall*, *Precision*, dan *F-1 Score* masing-masing pada model *Random Forest* dan KNN dalam mengklasifikasi serangan DDoS dengan melihat tingkat akurasi yang di dapatkan.

1.6 Manfaat Penelitian

Berdasarkan rumusan masalah, batasan masalah dan tujuan penelitian yang telah diuraikan di atas, maka dapat diketahui manfaat dari penelitian ini adalah:

1. Manfaat Praktis

a. Bagi Peneliti, memperoleh keterampilan dalam pengembangan dan penerapan beberapa model *Machine Learning* yaitu KNN dan *Random Forest*.

b. Bagi masyarakat, ,memberi kemudahan dalam membedakan serangan DDoS yang asli dengan keadaan *server* sedang sibuk melayani klien.

c. Bagi Institut Teknologi Telkom Purwokerto, dapat meningkatkan dasar pengetahuan tentang *Machine Learning* yang cocok digunakan dalam mendeteksi sebuah serangan DDoS.

2. Manfaat Teoritis

a. Bagi Peneliti, memperoleh pemahaman tentang bagaimana cara kerja dari masing-masing *Machine Learning* yang digunakan.

b. Bagi Masyarakat, meningkatkan pengetahuan dan kemampuan dalam membedakan klien asli dengan serangan DDoS.

c. Bagi Institut Teknologi Telkom Purwokerto, hasil penelitian ini dapat menjadi referensi penelitian selanjutnya untuk membangun sebuah sistem yang melibatkan pendeteksi serangan DDoS.