BAB 1
PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi informasi saat ini sangat pesat di berbagai sektor karena memiliki keuntungan yaitu peningkatan produktivitas, kualitas, kondisi kerja, transparansi proses, dan model bisnis yang menguntungkan, situs web merupakan salah satu pemanfaatan teknologi informasi yang digunakan sebagai sarana media informasi, promosi, tempat bertransaksi, dan hiburan [1].

Dibalik pesatnya penggunaan teknologi informasi terdapat ancaman serangan oleh orang yang tidak bertanggung jawab yang berusaha merusak sistem, menurut data laporan pemantauan Badan Siber dan Sandi Negara (BSSN) pada tahun 2021 tercatat terjadi serangan *web defacement* sebesar 5.940 kasus dengan sektor yang paling terdampak terdapat pada sektor akademik yang dalam hal ini perguruan tinggi dengan 2.217 kasus, kemudian di urutan kedua ada perusahaan swasta dengan 1.483 kasus, dilanjutkan ketiga yaitu pemerintah daerah dengan 1.097 kasus dan keempat yaitu pemerintah pusat dengan 477 kasus [2].

Salah satu jenis *cyber attack* yang paling sering dijumpai adalah DDoS, DDoS *(Distributed Denial of Service)* merupakan metode penyerangan yang sering terjadi pada server web, pada DDoS tidak memiliki tujuan untuk mencuri atau membocorkan data melainkan untuk merusak sistem dengan cara membanjiri *traffic* palsu pada server web target dan membuat server menjadi sibuk dengan banyaknya permintaan layanan sehingga dapat menurunkan performa bahkan membuat server web menjadi *down*[3].

Pada penerepannya untuk mendeteksi serangan DDoS membutuhkan sebuah sistem IDS *(Intrusion Detection System)* yaitu sebuah sistem yang digunakan untuk mendeteksi dan melaporkan serangan siber atau aktivitas yang tidak diinginkan pada jaringan komputer dengan cara memantau aktivitas *traffic jaringan* secara *realtime* dan dapat memberikan notifikasi atau alarm peringatan yang digunakan

untuk mengambil tindakan preventif atau tindakan korektif dalam mengatasi serangan tersebut [4].

Namun, seiring berkembangnya zaman dan pesatnya kemajuan infrastruktur jaringan serangan DDoS menjadi lebih canggih dan serangan yang dihasilkan pun juga semakin kuat dengan MTU *(Maximum Transmission Unit)* [5]. Maka dari itu diperlukannya sebuah pengembangan dan pembaruan teknologi yang diterapkan untuk meningkatkan akurasi deteksi serangan DDoS ini yaitu dengan teknologi *Machine Learning* [6]. *Machine Learning* adalah cabang dari ilmu komputer yang berfokus pada pembuatan sistem yang dapat belajar dan mengambil keputusan tanpa diberi instruksi yang spesifik [7].

Sudah terdapat penelitian sebelumnya yang membahas mengenai sistem deteksi serangan DDoS menggunakan *machine learning*. Pada penelitian yang dilakukan Wani et al. [8] tahun 2019 yang berjudul *Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques* melakukan percobaan deteksi DDoS dengan metode *Random Forest* menghasilkan nilai akurasi terhadap serangan DDoS *(Distributed Denial of Service)* sebesar 98%.

Selanjutnya terdapat penelitian yang dilakukan Chen et al. [9] pada tahun 2020 yang berjudul *DDoS Attack Detection Based on Random Forest* menggunakan algoritma *random forest* untuk mendeteksi serangan DDoS dengan dataset yang digunakan berjumlah 4 yaitu *LLDoS1.0, LLDoS2.0.1, UDP Flood Attack* dan *ICMP Flood Attack* menghasilkan tingkat akurasi sebesar 99.41%.

Lalu pada penelitian yang dilakukan Alduailij et al. [10] pada tahun 2022 mereka melakukan uji coba deteksi serangan DDoS dengan membandingkan 5 algoritma machine learning yaitu *Gradient Boosting,* KNN, *Logistic Regression, Random Forest* dan *Weighted Voting Ensemble* untuk mendeteksi serangan DDoS dengan hasil algoritma *Random Forest* memiliki tingkat akurasi yang paling tinggi dengan nilai akurasi sebesar 99,7%

Pada penelitian yang dilakukan Vimal Gaur Rajneesh Kumar pada tahun 2022 mereka melakukan ujiocoba deteksi serangan DDoS dengan menggunakan dataset CICDDoS-2019. Metode pemilihan fitur yaitu chi-square, Extra Tree dan ANOVA telah diterapkan pada empat klasifikasi Random Forest, Decision Tree, k-Nearest

Neighbors dan XGBoost untuk deteksi dini serangan DDoS pada perangkat IoT, didapatkanlah hasil akurasi sebesar 98.34% [11].

Pada penelitian ini akan mencoba untuk melakukan percobaan deteksi serangan DDoS menggunakan algoritma *random forest* karena memiliki kelebihan yaitu memiliki tingkat akurasi yang tinggi dan efisiensi pada dataset [12]. Kemudian akan dilakukan optimasi terhadap algoritma *random forest* dengan menggunakan metode *bagging (Bootstrapped Aggregating)* yaitu metode yang menggunakan beberapa model yang dibangun dari *bootstrapping* pada dataset sehingga membantu mengurangi varians dari hasil model dan meningkatkan performa akurasi [13]. Untuk menghilangkan fitur yang tidak berguna dan berkontribusi minim terhadap model maka akan dilakukan optimasi dengan menggunakan metode *selection feature* dengan jenis yaitu *corelation-based Feature Selection* (CFS) yang mampu meningkatkan nilai akurasi deteksi serangan DDoS sebesar 99.784% dibandingkan dengan tanpa seleksi fitur yang hanya berkisar 49.501% [14].

Dari uraian latar belakang masalah yang telah penulis sampaikan, untuk memberikan sebuah kontribusi kepada ilmu pengetahuan terkhususnya pada bidang *cyber security* maka pada laporan tugas akhir ini akan membahas projek yang berjudul **"OPTIMASI PERFORMA ALGORITMA *RANDOM FOREST* MENGGUNAKAN METODE BAGGING DAN CFS *(CORRELATION-BASED FEATURE SELECTION)* UNTUK MENINGKATKAN AKURASI DETEKSI SERANGAN DDOS *(DENIAL DISTRIBUTED OF SERVICE)".***

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan sebelumnya, maka penulis mengemukakan beberapa rumusan masalah sebagai berikut :

1. Bagaimana cara meningkatkan akurasi deteksi serangan DDoS agar lebih baik dari penelitian yang telah dilakukan sebelumnya?
2. Bagaimana menerapkan metode bagging dan CFS *(Correlation-Based Feature Selection)* pada algoritma *Random Forest*?

1.3 Batasan Masalah

Untuk membatasi ruang lingkup permasalahan yang akan dibahas, maka dalam penulisan tugas akhir ini penulis lebih menekankan pada :

1. Algoritma *machine learning* yang digunakan dalam penelitian ini yaitu *Random Forest*.
2. Dataset yang akan digunakan bersifat publik yaitu CIC-DDOS2019.
3. Nilai akurasi akan dihitung menggunakan model *Confusion Matrix.*

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun berdasarkan rumusan masalah diatas maka tujuan dari penelitian tugas akhir ini yaitu :

1. Mendapatkan model *machine learning* yang mampu mendeteksi serangan DDoS dengan akurasi mendekati 100%.
2. Mampu mengetahui cara membuat sebuah model dengan optimasi pada algoritma *random forest* dalam rangka meningkatkan akurasi deteksi serangan DDoS.
3. Dapat mengetahui mengenai efektifitas performa akurasi model yang telah dioptimasi dibandingkan penelitian sebelumnya.

1.4.2 Manfaat

Adapun manfaat yang diperoleh jika tujuan dari penelitian tugas akhir ini dicapai yaitu :

1. Dapat memberikan kontribusi kepada ilmu pengetahuan teknologi khususnya dibidang *cyber security* dalam mendeteksi serangan DDoS.
2. Dapat membantu pemerintah, organisasi, dan masyarakat dalam menangani kasus *cyberattack* khususnya DDoS pada pengaplikasian model deteksi.
3. Dapat memberikan solusi model *machine learning* dengan akurasi yang tinggi untuk mendeteksi serangan DDoS.

1.5 Metode Penulisan

Untuk mempermudah penulisan dalam penyusunan proposal tugas akhir, maka penulis menggunakan metode – metode sebagai berikut :

1.5.1 Metode Studi Literatur

Metode studi literatur merupakan metode yang digunakan penulis dalam medapatkan teori-teori yang akan dibahas dengan mengumpulkan semua referensi-referensi yang berhubungan dengan laporan yang akan dibuat. Pada referensi tersebut dapat diperoleh dari teori-teori dasar pada studi kepustakaan yang diberikan pembimbing maupun buku-buku dan media lain seperti internet sebagai landasan dalam menyusun proposal tugas akhir.

1.5.2 Metode Konsultasi

Metode konsultasi merupakan metode yang digunakan penulis dalam melakukan interaksi dengan meminta saran, masukan, atau solusi terhadap masalah yang dihadapi kepada dosen pembimbing. Tujuan dari metode konsultasi adalah untuk meminta bantuan menemukan solusi terbaik untuk masalah yang dihadapi, dan mendorong mengembangkan kemampuan dan kepercayaan diri dalam menyelesaikan masalah.

1.5.3 Metode Observasi

Metode ini mengumpulan data dengan cara mengadakan secara teliti dan sistematis pada objek pembahasan dengan cara mengamati, menganalisa hubungan dengan topik yang dibahas. Observasi dimulai dengan pemantauan kebutuhan perangkat keras dan perangkat lunak apa saja yang diperlukan untuk mencapai tujuan dalam mengimplementasikan sistem yang diharapkan.

1.6 Sistematika Penulisan

Di dalam pembuatan suatu karya tulis, dibutuhkan suatu sistematika penulisan agar pembaca dapat mempermudah dalam memahami dan membaca isi dari tugas akhir ini. Adapun penulisan proposal tugas akhir ini terdiri atas 4 empat bab, yang dapat dikemukan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini, penulis memberikan gambaran secara jelas mengenai latar belakang permasalahan, ruang lingkup masalah, maksud dan tujuan, metodologi penulisan dan sistem penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini membahas tentang informasi yang bersifat umum dan merupakan teori pendukung pada pembahasan masalah berdasarkan referensi serta penelitian sebelumnya yang berkaitan dengan tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Pada bab ini membahas mengenai kerangka penelitian, perancangan sistem yang akan dibuat, pengembangan metode, serta kinerja sistem penelitian tugas akhir ini.

BAB IV HASIL YANG DIHARAPKAN

Pada bab ini menjelaskan hasil yang akan dicapai dengan menggunakan metodologi yang telah ditentukan sebelumnya. Bab ini juga merencanakan waktu yang dibutuhkan dalam perancangan sistem.