BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang sangat pesat telah memberikan dampak besar terhadap berbagai aspek kehidupan manusia, mulai dari sektor pemerintahan, bisnis, hingga pendidikan. Pemanfaatan jaringan komputer dan internet memungkinkan pertukaran informasi secara cepat dan efisien, sehingga aktivitas digital menjadi semakin terintegrasi dalam kehidupan sehari-hari. Namun, perkembangan tersebut juga membawa tantangan baru dalam aspek keamanan siber. Menurut Stallings (2018), meningkatnya jumlah perangkat dan konektivitas jaringan berbanding lurus dengan meningkatnya risiko ancaman keamanan terhadap ketersediaan dan integritas layanan jaringan. Salah satu ancaman yang paling sering terjadi dan merugikan adalah serangan Denial of Service (DoS) serta Distributed Denial of Service (DDoS), di mana penyerang berusaha melumpuhkan layanan dengan mengirimkan lalu lintas data berlebih atau palsu yang menyebabkan sistem tidak dapat diakses oleh pengguna sah.[1]

Serangan *DDoS* kini menjadi salah satu tantangan paling serius dalam bidang keamanan jaringan karena sifatnya yang terdistribusi, sulit dideteksi, serta menyerang dari berbagai sumber secara bersamaan. Pola serangan yang mirip dengan lalu lintas normal menyebabkan metode pertahanan seperti *firewall* dan *Intrusion Detection System (IDS)* menjadi kurang efektif dalam mendeteksi serangan modern Akibatnya, banyak sistem jaringan mengalami penurunan kinerja dan bahkan gangguan total yang berimbas pada kerugian finansial dan reputasi organisasi. Oleh karena itu, pendekatan berbasis kecerdasan buatan dan *machine learning* mulai banyak digunakan karena kemampuannya dalam mengenali pola anomali trafik secara adaptif dan real time. Pengembangan metode deteksi yang cerdas dan akurat menjadi langkah penting untuk meningkatkan keamanan dan stabilitas layanan digital di era transformasi teknologi yang semakin maju [2]

Berbagai penelitian telah mengembangkan metode klasifikasi serangan *DoS* dan *DDoS* dengan memanfaatkan algoritma *machine learning* untuk meningkatkan akurasi serta efisiensi dalam proses identifikasi serangan. Menurut penelitian berjudul *"Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method" (2022)* kombinasi antara pemilihan fitur berbasis mutual information dan algoritma *Random Forest* mampu meningkatkan performa deteksi karena *RF* memiliki kemampuan dalam menangani data berukuran besar serta melakukan klasifikasi secara akurat tanpa mengalami *overfitting*. Dalam penelitian tersebut, *Random Forest* menunjukkan tingkat akurasi yang lebih baik dibandingkan beberapa metode konvensional lain seperti *Naive Bayes* dan *K-Nearest Neighbor*. Hal ini disebabkan oleh mekanisme *ensemble learning* pada *Random Forest* yang menggabungkan beberapa *decision tree* untuk menghasilkan prediksi yang lebih stabil dan konsisten terhadap pola serangan yang kompleks [3]

Sementara itu, penelitian berjudul *"Evaluation of DoS/DDoS Attack Detection with ML Techniques on CIC-IDS2017 Dataset"* (2023) mengevaluasi performa beberapa algoritma *Machine Learning* pada dataset CICIDS2017 dalam mendeteksi serangan *DoS* dan *DDoS*. Hasilnya menunjukkan bahwa *Support Vector Machine (SVM)* memiliki tingkat presisi dan recall yang tinggi dalam memisahkan data serangan dan normal, terutama pada data berdimensi tinggi. *SVM* mampu menentukan batas optimal antar kelas dengan margin maksimum, sehingga efektif untuk mendeteksi trafik jaringan yang sulit dikenali oleh metode *signature-based*. Berdasarkan hasil penelitian-penelitian tersebut, pemilihan algoritma *Random Forest* dan *SVM* dalam penelitian ini dianggap tepat karena keduanya terbukti memiliki performa unggul dalam mendeteksi serangan *DDoS* secara akurat dan efisien [4]

Penelitian ini bertujuan untuk mendeteksi serangan *DoS* dan *DDoS* menggunakan pendekatan berbasis *machine learning* dengan algoritma *Random Forest (RF)* dan *Support Vector Machine (SVM)*. Metode penelitian diawali dengan tahap pengumpulan dan pra-pemrosesan data dari dataset serangan jaringan

(misalnya CICIDS2017), dilanjutkan dengan ekstraksi dan seleksi fitur untuk memperoleh atribut paling relevan terhadap pola serangan. Tahap berikutnya adalah pelatihan model *RF* dan *SVM* dengan membagi data menjadi data latih dan uji, kemudian dilakukan evaluasi performa menggunakan parameter *accuracy, precision, recall,* dan *F1-score* untuk mengukur efektivitas masing-masing algoritma.

Pengujian dilakukan untuk membandingkan kemampuan kedua model dalam mengenali pola serangan *DDoS* secara dini serta membedakannya dari trafik normal jaringan. Hasil penelitian diharapkan mampu menunjukkan bahwa kombinasi *RF* dan *SVM* dapat meningkatkan akurasi deteksi serta mengurangi tingkat kesalahan klasifikasi. Selain itu, sistem yang dikembangkan diharapkan dapat menjadi model deteksi yang adaptif, efisien, dan mudah diimplementasikan pada lingkungan jaringan nyata guna memperkuat keamanan infrastruktur digital terhadap ancaman serangan *DoS* dan *DDoS*.

1.2 Rumusan Masalah

Serangan jaringan seperti Denial of Service (DoS) dan Distributed Denial of Service (DDoS) merupakan ancaman serius terhadap ketersediaan dan stabilitas sistem jaringan komputer. Oleh karena itu, diperlukan pendekatan berbasis *machine learning* yang mampu mengklasifikasikan dan mengidentifikasi pola serangan secara lebih akurat dan efisien. Dalam penelitian ini digunakan algoritma Random Forest dan Support Vector Machine (SVM) untuk mendeteksi serangan DoS/DDoS serta mengklasifikasikan lalu lintas jaringan menjadi kategori normal dan berbahaya.

Berdasarkan latar belakang tersebut, dirumuskan permasalahan penelitian agar pembahasan lebih terarah, dengan fokus pada analisis dan perbandingan kinerja algoritma Random Forest dan SVM dalam mendeteksi serangan DoS/DDoS.

1. Bagaimana cara mendeteksi serangan jaringan *DoS/DDoS* menggunakan algoritma *Random Forest* dan *Support Vector Machine (SVM)*?

2. Algoritma manakah di antara *Random Forest* dan *Support Vector Machine (SVM)* yang memiliki akurasi dan performa terbaik dalam mendeteksi serangan jaringan *DoS/DDoS*?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah dijelaskan sebelumnya, agar penelitian ini lebih terarah dan fokus, maka ditetapkan beberapa batasan masalah sebagai berikut:

1. Jenis serangan yang dikaji dalam penelitian ini hanya mencakup serangan *Denial of Service (DoS)* dan *Distributed Denial of Service (DDoS)*, tanpa membahas jenis serangan siber lainnya seperti *phishing, malware, ransomware*, atau *SQL injection*.

2. Metode klasifikasi yang digunakan terbatas pada algoritma *Random Forest* dan *Support Vector Machine (SVM)* sebagai pembanding dalam mendeteksi trafik serangan jaringan. Algoritma lain seperti *Decision Tree, Naïve Bayes*, atau *K-Nearest Neighbor* tidak termasuk dalam ruang lingkup penelitian ini.

3. Dataset yang digunakan adalah CIC-IDS2017, yang berisi data lalu lintas jaringan normal dan serangan *DoS/DDoS*. Tidak dilakukan proses pengumpulan data baru maupun pembuatan dataset sintetis.

4. Evaluasi performa model difokuskan pada analisis metrik *accuracy, precision, recall*, dan *F1-score*, tanpa mempertimbangkan aspek efisiensi komputasi seperti waktu pelatihan atau penggunaan memori secara mendalam.

5. Lingkungan pengujian dilakukan secara simulasi menggunakan bahasa *Python* dengan bantuan *library Scikit-learn*, tanpa implementasi langsung pada perangkat keras jaringan (*network devices)* atau sistem produksi nyata.

6. Faktor eksternal seperti perubahan konfigurasi jaringan, variasi hardware, kondisi lalu lintas jaringan real-time, serta pengaruh skala jaringan besar tidak dibahas secara mendalam karena berada di luar fokus penelitian ini.

7. Proses penelitian hanya difokuskan pada tahap deteksi serangan *(attack detection)* untuk mengidentifikasi adanya aktivitas anomali, tanpa melibatkan tahap mitigasi, respon otomatis, atau pemulihan sistem *(recovery)* setelah serangan terdeteksi.

1.4 Tujuan Penelitian

Penelitian ini dilakukan untuk menjawab permasalahan yang telah dirumuskan sebelumnya, khususnya terkait efektivitas penerapan algoritma *machine learning* dalam mendeteksi serangan jaringan *DoS* dan *DDoS*. Melalui pendekatan komparatif antara algoritma *Random Forest* dan *Support Vector Machine (SVM)*, penelitian ini bertujuan untuk menganalisis performa kedua metode tersebut dalam mengidentifikasi pola serangan jaringan secara akurat dan efisien.

Tujuan penelitian disusun untuk memberikan arah yang jelas serta menggambarkan hasil yang ingin dicapai. Tujuan ini juga menjadi dasar dalam penyusunan metode dan analisis penelitian. Adapun tujuan penelitian ini adalah sebagai berikut:

1. Untuk menganalisis dan membandingkan kinerja algoritma *Random Forest* dan *Support Vector Machine (SVM)* di dalam mendeteksi serangan jaringan *DoS (Denial of Service)* dan *DDoS (Distributed Denial of Service)*.
2. Untuk mengukur tingkat *accuracy, precision, recall,* dan *f1-score* dari kedua algoritma dalam proses klasifikasi trafik jaringan, menggunakan dataset CIC-IDS2017.
3. Untuk mengidentifikasi kelebihan dan kekurangan masing-masing algoritma *machine learning* berdasarkan hasil pengujian yang dilakukan
4. Untuk menghasilkan model deteksi serangan *DoS/DDoS* berbasis *machine learning* yang efektif dan efisien dalam mengenali pola serangan jaringan secara otomatis.
5. Untuk memberikan rekomendasi metode deteksi serangan jaringan berbasis *machine learning* yang paling optimal dan dapat dijadikan dasar

dalam pengembangan sistem keamanan jaringan di masa mendatang.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi yang signifikan baik secara teoritis maupun praktis dalam bidang keamanan jaringan komputer, khususnya dalam mendeteksi dan menganalisis serangan *DoS* dan *DDoS* menggunakan algoritma *machine learning*. Dengan adanya penelitian ini, diharapkan dapat membantu meningkatkan serta menambah pemahaman terhadap penerapan metode klasifikasi cerdas untuk keamanan siber. Penelitian ini diharapkan memberikan kontribusi baik secara teoritis maupun praktis. Manfaat tersebut dirumuskan untuk menunjukkan nilai tambah penelitian terhadap bidang keamanan jaringan serta implementasinya pada sistem nyata. Adapun manfaat penelitian ini meliputi:

1. Manfaat Teoritis

Secara teoritis, penelitian ini dapat menambah wawasan dan pengetahuan dalam bidang keamanan jaringan berbasis *machine learning*. Dari hasil penelitian ini diharapkan dapat menjadi referensi ilmiah bagi penelitian selanjutnya yang ingin mengembangkan model deteksi serangan jaringan dengan kombinasi algoritma lainnya atau dengan menggunkan dataset yang berbeda. Penelitian ini juga memperkuat bukti empiris tentang efektivitas algoritma *Random Forest* dan *Support Vector Machine* dalam menganalisis lalu lintas jaringan yang mengandung serangan *DoS/DDoS*.

2. Manfaat Praktis

Secara praktis, penelitian ini dapat menjadi acuan bagi pengelola sistem jaringan, dalam mengimplementasikan sistem deteksi serangan yang lebih efisien dan akurat. Dengan memanfaatkan model yang dikembangkan sehingga dapat mempercepat proses identifikasi serangan dan meminimalkan dampak gangguan terhadap layanan jaringan. Hasil penelitian ini juga dapat digunakan sebagai dasar yang untuk pengembangan *Intrusion Detection System (IDS)* berbasis pembelajaran

mesin lebih adaptif di masa mendatang.

1.6 Sistematika Penulisan

Untuk memberikan gambaran mengenai susunan isi laporan skripsi ini, berikut disajikan sistematika penulisan yang terdiri dari lima bab utama. Setiap bab memiliki fokus pembahasan masing-masing. Sistematika penulisan skripsi ini disusun agar pembahasan dalam penelitian menjadi lebih terarah dan mudah dipahami. Adapun sistematika penulisan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi uraian mengenai latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan. Bab ini memberikan gambaran umum mengenai alasan dan arah penelitian terkait deteksi serangan jaringan *DoS/DDoS* menggunakan algoritma *Random Forest* dan *Support Vector Machine (SVM)*.

BAB II TINJAUAN PUSTAKA

Pada bab ini membahas dasar teori dan konsep yang mendukung penelitian, termasuk penjelasan tentang serangan *DoS/DDoS*, konsep keamanan jaringan, prinsip kerja algoritma *Random Forest* dan *Support Vector Machine (SVM)*, serta penelitian-penelitian terdahulu yang relevan. Selain itu, bab ini juga memuat kerangka teori dan kerangka berpikir yang menjadi landasan penelitian.

BAB III METODE PENELITIAN

Bab ini menjelaskan metode yang digunakan dalam penelitian, meliputi objek penelitian, data dan sumber data, yaitu dataset CIC-IDS2017, serta tahapan penelitian. Pada bab ini juga dijelaskan proses penerapan algoritma *Random Forest dan SVM* untuk mendeteksi serangan *DoS/DDoS* menggunakan dataset CIC IDS2017 serta metode evaluasi performa model.

BAB IV HASIL DAN PEMBAHASAN

Di dalam bab ini menyajikan hasil pengujian dan analisis dari penerapan algoritma *Random Forest* dan *SVM* dalam mendeteksi serangan *DoS/DDoS*.

Pembahasan meliputi perbandingan kinerja kedua algoritma berdasarkan metrik evaluasi seperti *accuracy, precision, recall,* dan *f1-score*, serta interpretasi hasil yang diperoleh.

BAB V PENUTUP

Pada bab kelima ini berisi kesimpulan yang diperoleh dari hasil penelitian dan pembahasan, serta saran yang dapat dijadikan acuan untuk pengembangan penelitian selanjutnya, khususnya dalam peningkatan performa deteksi serangan jaringan menggunakan metode *machine learning*.

Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem deteksi serangan jaringan yang lebih efektif melalui penerapan algoritma *machine learning*, khususnya *Random Forest* dan *Support Vector Machine (SVM)*.