BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam era konektivitas digital yang semakin meningkat ini, sistem dan jaringan komputer telah menjadi landasan utama bagi banyak aspek kehidupan dan bisnis. Sayangnya, keamanan siber semakin menjadi tantangan dengan munculnya berbagai serangan, termasuk Serangan Distributed Denial of Service (DDoS). Selama beberapa tahun terakhir banyak situs di Internet telah target serangan Distributed Denial of Service (DDoS)[1]. Serangan DDoS menciptakan lonjakan lalu lintas yang luar biasa pada suatu sistem atau jaringan, bertujuan untuk mengeksploitasi dan merugikan layanan yang tersedia bagi pengguna[2].

Serangan DDoS merujuk pada jenis serangan yang melibatkan sejumlah sistem komputer yang diretas untuk menyerang suatu target, seperti server, sumber daya apapun, dan situs web. Akibatnya, layanan kepada pengguna akhir dan sumber daya yang menjadi target dapat ditolak. Taktik yang digunakan melibatkan pengiriman permintaan koneksi palsu, pengiriman pesan masuk secara berlebihan, atau manipulasi paket data, yang secara kolektif menyebabkan sistem keseluruhan menjadi lambat atau bahkan mengalami kegagalan, mengakibatkan penolakan layanan bagi pengguna akhir dan sistem yang menjadi sasaran[3]. Dampak dari serangan DDoS meliputi ketidakmampuan mengakses layanan, penurunan kinerja sistem, dan bahkan potensi merusak reputasi suatu organisasi. Oleh karena itu, mendesak dibutuhkan sistem keamanan yang mampu mendeteksi dan merespons serangan DDoS untuk melindungi integritas dan ketersediaan layanan[4].

Serangan DDoS merupakan ancaman serius dalam dunia siber yang dapat menyebabkan kerugian besar bagi organisasi dan infrastruktur sehingga terdapat berbagai pendekatan yang ada untuk menghindari serta mendeteksi serangan DDos seperti Deteksi Berbasis Tanda Tangan (Signature-Based Detection) yang melibatkan penggunaan tanda tangan atau pola yang telah diketahui dari serangan DDoS sebelumnya untuk mengidentifikasi serangan serupa dalam lalu lintas jaringan[5]. Sistem *Intrusion Prevention System* (IPS) atau *Firewall* yang membandingkan lalu lintas dengan *database* tanda tangan yang telah ada[6]. Serta Pemodelan dan Pembelajaran Mesin yang digunakan untuk mempelajari pola lalu lintas normal dan membedakan antara lalu lintas normal dan serangan DDoS.

Algoritma seperti *Decision Trees*, *Random Forest*, *Support Vector Machines* (SVM), atau *Isolation Forest* dapat digunakan untuk mengidentifikasi serangan DDoS.

Dalam konteks deteksi serangan DDoS, algoritma pembelajaran mesin menjadi populer karena kemampuannya untuk mempelajari pola data yang kompleks dan mendeteksi anomali. Dua algoritma yang sering digunakan untuk deteksi anomali adalah *Support Vector Machines* (SVM)[7] dan *Isolation Forest*[8]. SVM merupakan algoritma yang telah terbukti efektif dalam klasifikasi dan regresi. Dalam mendeteksi anomali, SVM bekerja dengan mencari *hyperplane* yang memisahkan data normal dari data anomali dalam ruang fitur. SVM memaksimalkan margin antara *hyperplane* dan titik data terdekat, sehingga memungkinkan untuk mengidentifikasi data yang jauh dari *hyperplane* sebagai anomali[9]. Sedangkan *Isolation Forest* adalah algoritma yang dikembangkan khusus untuk deteksi anomali. Pendekatan ini bekerja dengan membangun pohon isolasi secara acak dari data, di mana titik data anomali cenderung memiliki jalur yang lebih pendek untuk diisolasi dalam pohon dibandingkan dengan data normal. Dengan mengukur jumlah pemisahan yang diperlukan untuk mengisolasi titik data, *Isolation Forest* dapat mengidentifikasi anomali dengan cepat dan efisien[10].

Penelitian yang dilakukan oleh Li menunjukan bahwa algoritma SVM memiliki tingkat deteksi yang lebih tinggi dibandingkan metode deteksi tradisional, namun sangat dipengaruhi oleh pemilihan kumpulan data awal dan memakan waktu yang lama sehingga kurang efektif[11]. Hasil penelitian menunjukkan bahwa *Isolation Forest* sering kali memiliki keunggulan dalam mendeteksi anomali, terutama ketika data memiliki dimensi tinggi dan terdapat banyak fitur yang tidak relevan. Selain itu, *Isolation Forest* cenderung lebih efisien secara komputasional daripada SVM dalam beberapa situasi. Salah satu keunggulan *Isolation Forest* adalah fleksibilitasnya dalam menangani data yang besar dan kompleks, serta kemampuannya untuk mengidentifikasi anomali tanpa memerlukan data pelatihan yang terlalu banyak. Di sisi lain, SVM dapat menjadi lebih sulit untuk diterapkan dan memerlukan tuning parameter yang lebih rumit terutama dalam kasus data yang besar.

Deteksi anomali merupakan salah satu pendekatan penting untuk mengidentifikasi perilaku yang tidak biasa dalam data atau jaringan. Algoritma *Isolation Forest* secara khusus dirancang untuk mendeteksi anomali dengan mengisolasi instansi atau titik data yang langka[12]. Pendekatan ini didasarkan pada ide bahwa anomali umumnya memerlukan jumlah atribut yang lebih sedikit untuk diisolasi daripada titik data normal. Keunggulan utama dari algoritma *Isolation*

Forest adalah kemampuannya dalam menangani data tinggi dimensi dengan efisien, serta kemampuannya untuk mendeteksi anomali tanpa memerlukan data pelatihan yang terlalu banyak sehingga cocok dalam deteksi serangan siber, di mana data seringkali kompleks dan terus berubah. Dalam konteks deteksi serangan DDoS, algoritma *Isolation Forest* sangat berguna karena dapat mengidentifikasi anomali dalam lalu lintas jaringan, sistem dapat memberikan peringatan dini dan merespons secara cepat terhadap serangan DDoS, melindungi integritas dan ketersediaan sistem serta layanan yang disediakan[13]. Oleh karena itu, penelitian ini bertujuan untuk mendeteksi serangan DDoS dengan memanfaatkan keunggulan algoritma *Isolation Forest* sebagai bagian dari upaya meningkatkan keamanan jaringan dan melindungi infrastruktur siber dari ancaman yang semakin kompleks.

1.2 Rumusan Masalah

Rumusan masalah yang terbentuk dalam penelitian ini adalah:

a. Bagaimana mendeteksi anomali (serangan DDoS) dalam lalu lintas jaringan menggunakan algoritma *Isolation Forest* dan *One-Class SVM*?

b. Bagaimana kinerja algoritma *Isolation Forest* dan *One-Class SVM* dalam mendeteksi anomali pada lalu lintas jaringan, khususnya serangan DDoS?

1.3 Batasan Permasalahan

Penelitian ini membatasi cakupannya agar fokus pada deteksi anomali (serangan DDoS) menggunakan algoritma Isolation Forest. Adapun batasan-batasan yang diberlakukan dalam penelitian ini adalah:

a. Penelitian ini terbatas pada serangan DDoS konvensional yang melibatkan lonjakan lalu lintas, yaitu serangan *SYN flood*.

b. Sumber data yang digunakan adalah dataset lalu lintas jaringan yang mencakup situasi normal dan serangan DDoS yang didapat dari *https://www.kaggle.com/datasets/ymirsky/network-attack-dataset-kitsune/data*[14].

1.4 Tujuan Penelitian

Tujuan dari dilaksanakannya penelitian ini dilakukan adalah:

a. Mendeteksi anomali (serangan DDoS) dalam lalu lintas jaringan menggunakan algoritma *Isolation Forest* dan *One-Class SVM*.

b. Mengetahui kinerja algoritma *Isolation Forest* dan *One-Class SVM* dalam mendeteksi anomali pada lalu lintas jaringan, khususnya serangan DDoS.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

a. Memberikan kontribusi pada pengembangan teknologi keamanan jaringan dengan memperkenalkan algoritma pendeteksi anomali (serangan DDoS) yang efektif dan adaptif.

b. Mengoptimalkan kinerja deteksi dengan memanfaatkan algoritma *Isolation Forest* dan *One-Class SVM* dalam mendeteksi anomali pada lalu lintas jaringan.

1.6 Sistematika Penulisan

Sistematika penulisan laporan adalah sebagai berikut:

a. Bab 1 PENDAHULUAN
   Bab ini berisikan latar belakang penelitian, rumusan masalah, batasan permasalahan, serta tujuan dan manfaat dari penelitian yang dilakukan.

b. Bab 2 LANDASAN TEORI
   Bab ini berisikan tinjauan teori yang menjelaskan teori-teori yang digunakan sebagai dasar pengetahuan dalam penelitian seperti teori *Distributed Denial of Service* (DDoS), Anomali, *Machine Learning*, *Supervised vs Unsupervised Machine Learning*, algoritma *Isolation Forest*, *One-Class SVM* (Support Vector Machine), dan *Confusion Matrix*.

c. Bab 3 METODOLOGI PENELITIAN
   Bab ini berisikan alur dan langkah-langkah dari penelitian yang dilakukan.

d. Bab 4 HASIL DAN DISKUSI
   Bab ini berisikan hasil serta analisis yang didapatkan dari penelitian yang dilakukan sesuai dengan metodologi.

e. Bab 5 KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan dari penelitian yang dilakukan serta saran untuk pembaca yang ingin melakukan penelitian serupa berikutnya.