BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi pada infrastruktur jaringan telah mengalami peningkatan yang signifikan dalam beberapa dekade terakhir. Namun, perkembangan ini juga berdampak pada meningkatnya risiko keamanan siber, dimana salah satu ancaman yang paling umum adalah serangan *Distributed Denial of Service* (DDoS). Serangan siber ini bertujuan untuk mengganggu ketersediaan dan kinerja server dengan cara membanjiri lalu lintas jaringan menggunakan data yang *overload*, sehingga sistem target tidak dapat diakses oleh pengguna yang sah (Afifah Rodhiyatun Nisa dkk., 2024).

Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN) dalam Lanskap Keamanan Siber Indonesia 2024, total anomali trafik yang terdeteksi mencapai 330 juta sepanjang tahun. Sebagian anomali tersebut merupakan indikasi serangan siber, dimana serangan DDoS termasuk dalam lima besar insiden yang paling sering terjadi. Serangan ini dapat berdampak terhadap performa perangkat dan jaringan, pencurian data sensitif, hingga merusak reputasi terhadap suatu instansi (BSSN, 2024).

Untuk mengatasi ancaman tersebut, *Intrusion Detection System* (IDS) merupakan metode yang digunakan dalam mendeteksi serangan siber dengan cara memantau lalu lintas jaringan dan mengidentifikasi aktivitas yang mencurigakan. Menurut Khaliq & Sari, (2022), IDS membantu administrator jaringan untuk mengenali jenis serangan dan melakukan tindakan mitigasi untuk meningkatkan keamanan sistem. Namun demikian, implementasi pendekatan yang digunakan IDS masih memiliki tantangan tersendiri. IDS berbasis tanda tangan (*signature-based*) memiliki keterbatasan dalam mengenali jenis serangan baru (*zero-day attack*), sedangkan pendekatan berbasis perilaku (*behavior-based*) lebih fleksibel dalam mendeteksi pola lalu lintas yang menyimpang, namun cenderung menghasilkan risiko *false positive* yang tinggi (Simanjuntak & Sijabat, 2024).

Kesalahan deteksi atau *false alarm* merupakan salah satu tantangan dalam IDS, yang mencakup *false positive* dan *false negative*. *False positive* terjadi ketika sistem mendeteksi suatu aktivitas normal pada lalu lintas jaringan sebagai serangan, sedangkan *false negative* terjadi ketika sistem tidak berhasil mendeteksi serangan yang sebenarnya (Gede dkk., 2024). Tantangan ini semakin kompleks dalam membedakan anomali dari lalu lintas normal, meskipun beberapa algoritma menunjukkan tingkat akurasi deteksi yang tinggi (Disha & Waheed, 2022).

Dalam upaya mengurangi tingkat *false alarm*, pendekatan berbasis *Machine Learning* (ML) telah banyak digunakan dalam penelitian terdahulu untuk mendeteksi anomali lalu lintas jaringan. ML melatih model menggunakan dataset historis untuk mengklasifikasikan lalu lintas normal atau serangan. Penelitian yang dilakukan oleh Wahyuni & Pitrasacha Adytia, (2022) membandingkan tiga algoritma ML, yaitu *XGBoost*, *Decision Tree*, dan *Artificial Neural Network* (ANN), meskipun menunjukkan akurasi deteksi yang tinggi, juga memiliki keterbatasan dalam efisiensi dan waktu eksekusi. Tingginya *false alarm* berdampak pada efektivitas sistem keamanan jaringan, sehingga diperlukan metode alternatif yang dapat meminimalkan hal tersebut.

Pendekatan yang digunakan dalam penelitian ini adalah metode Threshold-Based Detection, yaitu dengan menetapkan ambang batas (threshold) berdasarkan pola lalu lintas jaringan. Jika nilai metrik melebihi ambang batas yang telah ditentukan, maka sistem akan mengidentifikasi lalu lintas tersebut sebagai serangan (Sukma Aji dkk., 2024). Pada sebuah artikel disebutkan bahwa pendekatan ini umum digunakan untuk pemantauan *real-time* dibidang pemantauan jaringan dan sistem industri (JumpCloud, 2025). Tantangan utama dari pendekatan ini adalah menentukan ambang batas yang tepat agar dapat membedakan lalu lintas normal dan anomali secara akurat.

Untuk mengatasi permasalahan tersebut, digunakan teknik *unsupervised learning* seperti algoritma *Density-Based Spatial Clustering of Applications with Noise* (DBSCAN), yaitu algoritma yang mampu mengidentifikasi klaster dengan kepadatan data yang berbeda. Algoritma ini bekerja dengan dua parameter utama yaitu ε (*epsilon*) dan *MinPts* (Muhima dkk., 2021). Pada penelitan sebelumnya

menunjukkan bahwa DBSCAN memiliki *Silhouette Index* (SI) terbaik dibandingkan *K-Means* dan *Mean-Shift* (Cinderatama dkk., 2022). Selain itu, penelitian yang membandingkan metode *Naïve Bayes* dan DBSCAN memiliki hasil yang lebih baik dalam mendeteksi anomali lalu lintas jaringan (Bahtiar dkk., 2020).

Penelitian ini menggunakan dataset CIC-IDS2017 yang merepresentasikan lalu lintas normal (benign) dan berbagai jenis serangan, termasuk DDoS (Sharafaldin dkk., 2018). Meskipun dataset ini telah banyak digunakan, hasil yang diperoleh sering kali menunjukkan variasi yang signifikan. Misalnya, dalam suatu penelitian fitur tertentu dianggap sebagai anomali, sementara dalam penelitian lain dengan dataset yang sama, fitur tersebut diklasifikasikan sebagai normal (Engelen dkk., 2021). Hal tersebut menunjukkan bahwa belum ada nilai standar mengenai ambang batas deteksi, sehingga muncul kerancuan dan menimbulkan ambiguitas dalam mendeteksi serangan secara konsisten.

Berdasarkan hal tersebut, penelitian ini mengimplementasikan pendekatan threshold profiling, yaitu proses sistematis dalam menentukan nilai ambang batas berdasarkan karakteristik statistik atau distribusi data lalu lintas jaringan hasil *clustering*. Dalam hal ini, threshold profiling bertujuan untuk menentukan batas nilai dari fitur-fitur seperti *flow duration*, *flow packet/s*, atau *total bytes*. Apabila nilai tersebut melampui batas yang telah ditentukan, maka lalu lintas tersebut dapat diidentifikasi sebagai anomali. Fokus utama dalam penelitian ini adalah mendeteksi anomali yang merepresentasikan serangan DDoS, yang umumnya ditandai oleh lonjakan lalu lintas dalam durasi waktu yang singkat.

Oleh karena itu, penelitian ini mengusulkan pendekatan threshold profiling menggunakan DBSCAN pada dataset CIC-IDS2017, dengan tujuan mengkonstruksi nilai ambang batas yang lebih akurat dalam mendeteksi anomali serangan DDoS dalam lalu lintas jaringan.

1.2 Perumusan Masalah

Deteksi anomali serangan DDoS dalam lalu lintas jaringan masih menghadapi tantangan dalam akurasi deteksi, khususnya terkait tingginya *false alarm*. Pendekatan *Machine Learning* telah banyak digunakan, namun masih

menghasilkan *false positive* dan *false negative* yang cukup tinggi. Selain itu, meskipun dataset CIC-IDS2017 telah menjadi acuan dalam berbagai penelitian, hasil penelitian sering kali menunjukkan perbedaan signifikan karena variasi dalam *feature selection*, parameter algoritma, dan metode evaluasi.

Penelitian ini membatasi fokus pada penerapan metode *unsupervised learning* menggunakan algoritma DBSCAN dengan pendekatan threshold profiling untuk mendeteksi anomali serangan DDoS. Penelitian dibatasi pada penggunaan fitur-fitur statistik lalu lintas jaringan yang relevan terhadap serangan DDoS, seperti lonjakan volume dan kecepatan data. Penentuan threshold berdasarkan hasil *clustering* DBSCAN, untuk dapat mengidentifikasi anomali dan mengurangi *false alarm* serta tidak membandingkan secara langsung dengan metode *supervised learning*.

1.3 Pertanyaan Penelitian

1. Bagaimana pengaruh threshold profiling menggunakan DBSCAN terhadap akurasi deteksi anomali serangan DDoS?
2. Bagaimana efektivitas metode Threshold-Based Detection menggunakan DBSCAN dalam mengurangi *false alarm* pada deteksi anomali serangan DDoS?
3. Bagaimana penyesuaian parameter DBSCAN dalam efektivitas deteksi anomali serangan DDoS pada dataset CIC-IDS2017?

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk mengimplementasikan pendekatan threshold profiling menggunakan DBSCAN, guna mereduksi tingkat *false alarm* dalam deteksi anomali serangan DDoS pada dataset CIC-IDS2017.

1.5 Manfaat Hasil Penelitian

1. Meningkatkan akurasi deteksi anomali serangan DDoS dengan threshold profiling menggunakan DBSCAN.
2. Mengurangi tingkat *false alarm* dalam membedakan aktivitas normal dan ancaman yang sebenarnya.

3. Membantu pengelola keamanan jaringan dengan meminimalkan kesalahan deteksi yang memerlukan intervensi manual.
4. Menjadi referensi bagi penelitian selanjutnya dalam meningkatkan efektivitas sistem deteksi anomali berbasis Threshold-Based Detection.