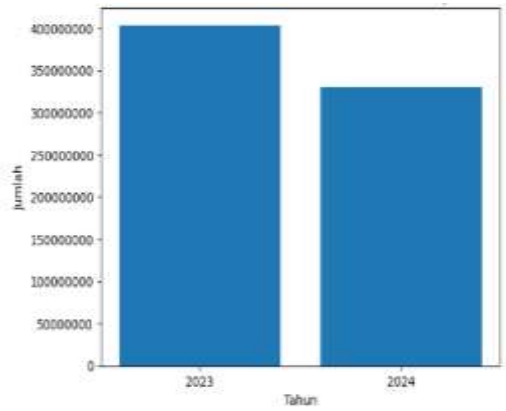
BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah memberikan dampak signifikan terhadap kemudahan akses dan pertukaran data dalam berbagai bidang. Namun, seiring meningkatnya penggunaan jaringan komputer, ancaman terhadap keamanan siber juga semakin kompleks dan beragam. Serangan seperti *Malware, Denial of Service (DoS), Probe, User to Root (U2R), Remote to Local (R2L),* dan lainnya terus berevolusi, menimbulkan resiko serius terhadap integritas, kerahasiaan, dan ketersediaan data.

Menurut Badan Siber dan Sandi Negara (BSSN), data statistik serangan siber baik secara global maupun diindonesia menunjukkan peningkatan yang signifikan setiap tahunnya baik dari sisi volume, intensitas, maupun kompleksitas serangannya (Badan Siber dan Sandi Negara., 2024) seperti pada gambar 1.1 di bawah ini.

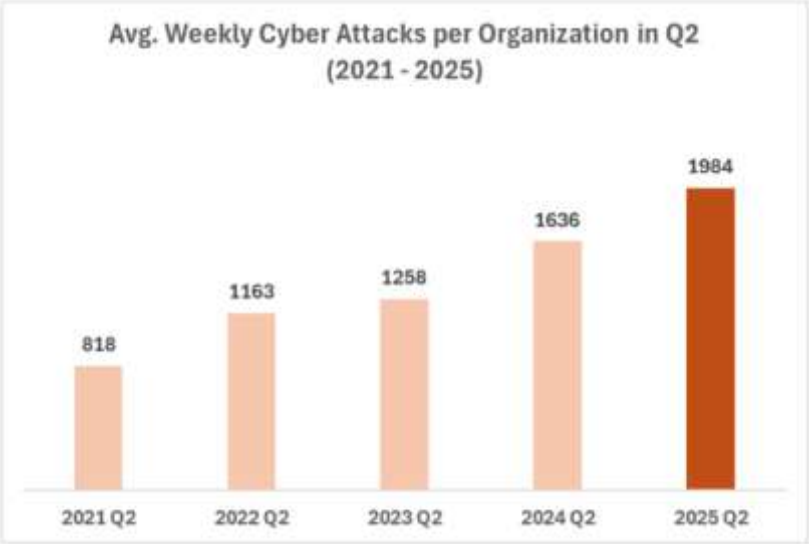


Gambar 1. 1 Grafik Total Serangan Siber
(Badan Siber dan Sandi Negara., 2024)

Gambar 1.1 menunjukkan bahwa pada tahun 2023, terdeteksi lebih dari 403 juta trafik anomali di ruang siber Indonesia, dan pada tahun 2024, total trafik anomali masih berada pada skala yang sangat besar yaitu sekitar 330 juta kejadian.

Pada gambar 1.2 menjelaskan statistik global pada laman website *cybersecurityasia.net* yang menunjukkan bahwa rata-rata jumlah serangan siber

mingguan yang dialami oleh setiap organisasi secara global pada kuartal kedua (Q2) dalam rentang waktu tahun 2021 hingga 2025 adalah sebagai berikut :



Gambar 1. 2 Grafik Total Serangan Siber secara Global
(Natalia Obregón Herráiz, 2025)

Gambar 1.2 menunjukkan peningkatan yang signifikan rata-rata serangan siber mingguan yang dialami oleh setiap organisasi secara global pada kuartal kedua (Q2) dengan angka tertinggi pada tahun 2025 yaitu 1.984 serangan perorganisasi perminggu. Besarnya jumlah trafik ini memberikan gambaran bahwa infrastruktur jaringan nasional menjadi target serangan yang terus menerus dan masif, dengan eskalasi ancaman siber yang konsisten dan berkelanjutan dari tahun ke tahun baik dari sisi frekuensi maupun intensitas serangan, sehingga membutuhkan mekanisme deteksi yang andal dan berkelanjutan. Kondisi ini menegaskan bahwa pendekatan keamanan tradisional yang hanya mengandalkan deteksi berbasis *signature* tidak lagi memadai dan menuntut adanya sistem pertahanan jaringan yang adaptif, cerdas dan mampu mengenali pola serangan secara efisien. Salah satu solusi yang banyak digunakan adalah *Intrusion Detection System* berbasis *machine learning*.

IDS berfungsi untuk mendeteksi aktivitas mencurigakan atau serangan dalam lalu lintas jaringan komputer. Snort merupakan salah satu IDS berbasis *signature* yang bersifat *open source* dan telah banyak digunakan karena kemampuannya mendeteksi pola serangan yang sudah diketahui (Antareza, 2024).

Namun, Snort memiliki keterbatasan yang cukup signifikan, terutama dalam mendeteksi serangan baru (*zero-day attack*) yang belum terdapat dalam basis data *signature* (*signature database*) sehingga memilki ketergantungan mutlak terhadap pembaruan database yang statis. Selain itu, pendekatan berbasis *signature* sering kali menghasilkan tingkat *false positive* yang tinggi yaitu kondisi dimana sistem keamanan memberikan peringatan serangan, padahal aktivitas yang terjadi normal dan tidak berbahaya (Antareza, 2024).

Sebagai alternatif, pendekatan *Machine learning* (ML) mampu memberikan paradigma baru dalam sistem deteksi intrusi. Dengan kemampuannya mempelajari pola dari data historis, ML dapat mengidentifikasi anomali maupun serangan baru yang belum terdefinisi sebelumnya. Salah satu algoritma ML yang banyak digunakan untuk klasifikasi adalah *Support Vector Machine* (SVM). SVM memiliki keunggulan dalam membedakan pola kompleks dengan tingkat akurasi tinggi, namun performanya sangat bergantung pada konfigurasi *tuning hyperparameter* yang optimal. Penggunaan konfigurasi default sering kali menghasilkan kinerja yang kurang maksimal karena tidak disesuaikan dengan karakteristik data tertentu.

Dalam penelitian ini, data log hasil deteksi Snort dianalisis menggunakan SVM *Machine learning*, dimana integrasi ini menghasilkan arsitektur *hybrid IDS* yang menggabungkan kekuatan deteksi *signature* dari Snort dan kemampuan klasifikasi adaptif dari SVM. Dengan melakukan optimasi tuning hyperparameter menggunakan metode *Grid search Cross Validation*, model mampu mengklasifikasikan berbagai jenis serangan seperti DoS, *probe scanning*, dan remote to local (R2L).

Berdasarkan permasalahan tersebut, penelitian ini mengembangkan ***Hybrid Intrusion Detection System*** dengan mengintegrasikan Snort dan SVM yang telah dioptimasi melalui penyesuaian *hyperparameter*, dengan fokus pada peningkatan akurasi klasifikasi, reduksi kesalahan deteksi, serta pembentukan sistem yang lebih cerdas dan adaptif terhadap pola serangan modern.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

10. Bagaimana meningkatkan efektifitas deteksi Snort terhadap variasi serangan jaringan?
11. Bagaimana mengoptimalkan performa *SVM machine learning* dalam klasifikasi jenis serangan jaringan?
12. Bagaimana merancang sistem *Hybrid IDS* berbasis integrasi Snort dan SVM Teroptimasi yang terukur dan dapat dievaluasi secara objektif?

1.3 Batasan Masalah

Agar ruang lingkup penelitian tidak terlalu luas, batasan masalah yang diterapkan adalah sebagai berikut:

1. Penelitian ini difokuskan pada model *Hybrid Intrusion Detection System* dengan mengintegrasikan snort dan algoritma SVM sebagai model klasifikasi membedakan jenis serangan jaringan. Integrasi hanya mencakup pemanfaatan output log Snort sebagai sumber data untuk proses klasifikasi.
2. Ruang lingkup optimasi terbatas pada penyesuaian *hyperparameter* SVM menggunakan metode Grid Search Cross Valudation yang bertujuan untuk meningkatkan akurasi klasifikasi dan kemampuan deteksi serangan jaringan.
3. Evaluasi kinerja model dilakukan melalui pengujian terhadap jenis serangan yang tersedia dalam data log Snort, dengan menggunakan metrik akurasi, presisi, recall, F1-score, serta tingkat *false positive* dan *false negative*.
4. Dataset dari simulasi IDS Snort ditraining dan ditesting untuk mandapatkan model terbaik yang diguanakan secara real-time pada server ubuntu.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

a. Mengintegrasikan Snort dan Algoritma SVM *machine learning* untuk membangun sistem deteksi intrusi yang lebih akurat dan adaptif dalam mengklasifikasikan jenis serangan

b. Melakukan optimasi performa model SVM melalui proses hyperparameter tuning menggunakan metode *Grid Search Cross Validation* untuk memperoleh kombinasi parameter terbaik dalam mengklasifikasikan serangan jaringan.
c. Mengembangkan model hybrid IDS yang menggabungkan kemampuan Snort berbasis *signature* dan SVM *machine learning* dengan melakukan evaluasi kinerja sistem menggunakan metrik evaluasi klasifikasi yaitu *Accuracy, precision, recall, f1-score*.

1.4.2 Manfaat

Adapun hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1.4.2.1 Manfaat Teoritis

a. Memberikan kontribusi dalam pengembangan model *Hybrid Intrusion Detection System* yang mengintegrasikan metode deteksi berbasis *signature* (Snort) dengan algoritma *machine learning Support Vector Machine* (SVM).
b. Memperkuat kajian akademik tentang pengaruh optimasi *hyperparameter* terhadap peningkatan kinerja SVM dalam klasifikasi serangan jaringan.
c. Menambah referensi penelitian terkait pendekatan hybrid dalam sistem keamanan jaringan yang mampu menangani keterbatasan metode deteksi tunggal.

1.4.2.2 Manfaat Praktis

1. Menyediakan model IDS yang lebih efektif dalam mendeteksi serangan, termasuk serangan baru yang belum terdaftar dalam *signature* database Snort.
2. Mengurangi tingkat *false positive* dan *false negative* yang sering muncul pada penggunaan IDS tradisional
3. Menjadi referensi implementatif bagi praktisi keamanan jaringan dalam meningkatkan kemampuan sistem pertahanan jaringan secara adaptif.

4. Memberikan hasil evaluasi yang mendalam sebagai dasar pengembangan atau penerapan sistem IDS yang lebih cerdas dan efisien.