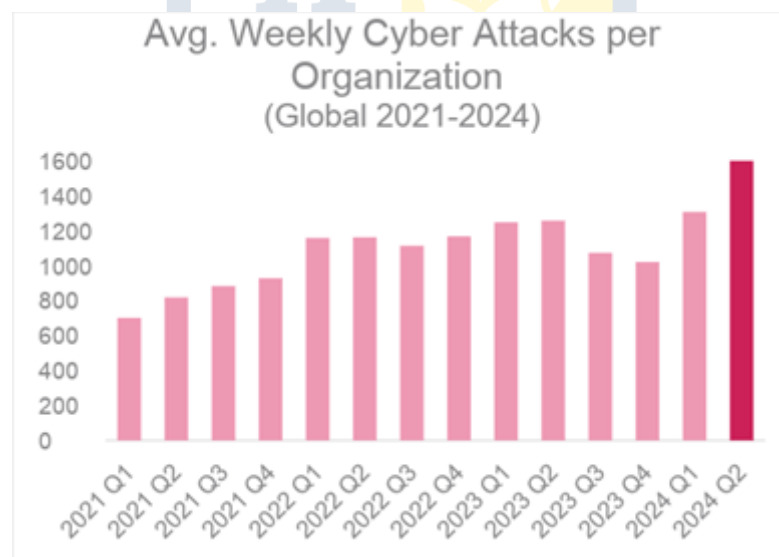


BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin berkembang, keamanan jaringan menjadi aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Meningkatnya jumlah perangkat yang terhubung ke internet serta kompleksitas infrastruktur jaringan telah membuka celah bagi berbagai jenis serangan siber. Beberapa jenis serangan siber yang umum terjadi diantaranya adalah *Distributed Denial of Service* (DDoS), *SQL Injection*, *Man-in-the-Middle* (MitM), serta serangan berbasis *malware* dan *ransomware*. Serangan tersebut dapat mengakibatkan pencurian data, gangguan layanan, hingga kerugian finansial bagi individu maupun kelompok.



Gambar 1. 1 Cyber Attack Statistics, 2024, Check Point [1]

Menurut laporan tahun 2024 (Gambar 1.1) oleh yang didapatkan dari berbagai lembaga keamanan siber, jumlah serangan siber yang terjadi di dunia semakin meningkat [1]. *Intrusion Detection System* (IDS) hadir sebagai salah satu solusi dalam menghadapi ancaman tersebut. IDS berperan untuk melakukan pemantauan terhadap lalu lintas jaringan dan mengidentifikasi aktivitas mencurigakan yang berpotensi sebagai ancaman keamanan. Di sisi lain, semakin

variatifnya pola - pola serangan siber membuat IDS juga harus berkembang. IDS konvensional yang berbasis aturan (*rule-based*) dan tanda tangan (*signature-based*) memiliki keterbatasan dalam menghadapi serangan yang semakin canggih sehingga pendeteksian yang dilakukan semakin tidak akurat, terlihat dari tingginya jumlah *false positive* dan *false negative*.

Maka dari itu, pengembangan model machine learning yang mampu menghadapi perkembangan serangan menjadi tantangan tersendiri. Perkembangan *deep learning* yang pesat memungkinkan penerapannya dalam pengembangan sistem deteksi serangan. Deep learning mampu mengenali pola - pola serangan yang sulit di deteksi oleh metode - metode konvensional seperti *rule-based* dan *signature-based*. Salah satu arsitektur deep learning yang lumrah digunakan untuk mengembangkan sistem untuk mendeteksi serangan siber adalah *Convolutional Neural Network* (CNN).

Convolutional Neural Network (CNN) adalah arsitektur deep learning yang telah terbukti efektif dalam menganalisis berbagai jenis data, termasuk teks, gambar, dan suara. Keunggulan utama CNN terletak pada kemampuannya untuk mengenali pola-pola kompleks dalam data melalui beberapa lapisan pemrosesan, seperti lapisan konvolusi dan pooling [2][3]. Selain CNN, metode Random Forest (RF) juga digunakan dalam sistem deteksi intrusi untuk meningkatkan akurasi klasifikasi. RF adalah algoritma machine learning berbasis ensemble yang terdiri dari banyak pohon keputusan (*decision trees*) dan bekerja dengan prinsip voting untuk menghasilkan keputusan akhir. Keunggulan utama RF terletak pada kemampuannya dalam menangani data yang kompleks serta mengurangi *overfitting* dibandingkan dengan model *decision tree* tunggal [4].

Sebagai respons terhadap tantangan tersebut, pendekatan berbasis *deep learning* telah berkembang pesat dalam bidang keamanan jaringan. *Deep learning* memungkinkan sistem untuk mengenali pola-pola anomali yang terdapat pada lalu lintas jaringan. Studi sebelumnya menunjukkan bahwa pendekatan berbasis *deep learning* ini dapat memberikan akurasi yang lebih tinggi dalam mendeteksi berbagai jenis serangan serta mengurangi terjadinya kesalahan deteksi.

Penelitian ini akan mengembangkan model machine learning untuk deteksi serangan siber menggunakan arsitektur CNN dan RF. Model *machine learning* yang dikembangkan akan bekerja berdasarkan data yang diambil dari file *packet capture* (PCAP) yang telah dikonversi menjadi format CSV. Di sisi lain, penelitian ini juga akan mengembangkan aplikasi berbasis web untuk memudahkan penggunaan dalam mengunggah file PCAP dan memperoleh hasil deteksi serangan siber.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, perumusan masalah pada penelitian ini adalah bagaimana mengembangkan model machine learning untuk mendeteksi serangan siber?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Ruang Lingkup Deteksi Serangan
 - Penelitian ini hanya berfokus pada pengembangan machine learning untuk mendeteksi serangan siber.
 - Tidak membahas metode keamanan jaringan lainnya seperti Intrusion Prevention System (IPS) atau firewall.
2. Jenis Serangan yang Dianalisis
 - Penelitian ini menggunakan dataset CICIDS2018 yang mencakup berbagai jenis serangan jaringan seperti DoS, *Botnet*, DDOS, dan *Infiltration Attack*.
 - Serangan yang tidak terdapat dalam dataset ini tidak menjadi fokus penelitian.
3. Metode yang Digunakan
 - Penelitian ini menggunakan penggabungan CNN dan RF sebagai model deep learning utama, tanpa membandingkannya dengan metode deep learning lainnya seperti Recurrent Neural Networks (RNN) atau Transformer.

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah yang telah dijelaskan, tujuan dari penelitian ini adalah untuk mengembangkan model machine learning untuk deteksi serangan siber.

1.5 Manfaat Penelitian

1. Manfaat Akademik

Manfaat akademik dari penelitian ini adalah untuk memberikan wawasan mengenai penerapan model machine learning untuk deteksi serangan siber.

2. Manfaat Praktis

Penelitian ini juga memberikan manfaat nyata bagi industri dalam bidang keamanan siber, yaitu:

- Dengan mengembangkan model machine learning untuk mendeteksi serangan siber, sistem dapat meningkatkan efektivitas deteksi serangan jaringan dengan cara mengenali pola serangan yang lebih akurat serta mengklasifikasikan serangan,
- Hasil dari penelitian ini dapat diterapkan oleh perusahaan atau penyedia layanan keamanan siber untuk memperkuat sistem deteksi terhadap ancaman jaringan

1.6 Sistematika Penelitian

BAB 1 PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang, identifikasi masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan yang berjudul “Pengembangan Model Machine Learning untuk Deteksi Serangan Siber”.

BAB 2 TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai teori teori yang mendukung pengembangan model *machine learning* untuk deteksi serangan siber. Termasuk, pengertian mengenai *machine learning*, *Convolutional Neural Networks (CNNs)*, *Random Forest (RF)*, *Deep Learning* dan semua teori pendukung lainnya yang berkaitan dengan penelitian ini.

BAB 3 METODOLOGI PENELITIAN

Bab ini menjelaskan tentang pembahasan secara detil dan lengkap mengenai tahapan yang dilakukan dalam proses pengembangan *machine learning* untuk deteksi serangan atau anomali jaringan menggunakan metode penggabungan *convolutional neural networks* dan *random forest*, seperti kerangka pemikiran, tahapan penelitian, dan hal-hal lain yang mendukung penelitian ini.

BAB 4 HASIL DAN EVALUASI

Bab ini menjelaskan hasil dan pembahasan mengenai output dari pengembangan model *machine learning* untuk deteksi serangan siber serta evaluasi penelitian ini.

BAB 5 SIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapat dan saran yang diberikan dari penelitian yang berjudul “Pengembangan Model *Machine Learning* untuk Deteksi Serangan Siber”

