202110370311338
Satria Milan Wicaksana
Prodi Informatika

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan semakin banyaknya perangkat yang terhubung dan meningkatnya volume data, kebutuhan akan arsitektur jaringan yang lebih maju semakin mendesak, baik melalui Internet of Things (IoT), komputer pribadi, maupun perangkat mobile. Dalam situasi ini, serangan DDoS (*Distributed Denial of Service*) telah menjadi ancaman bagi keamanan, integritas pada jaringan komputer serta sistem informasi [1]. DDoS merupakan jenis serangan yang berbahaya, karena dapat membanjiri jaringan dan menghentikan akses ke server dengan mengirimkan sejumlah besar paket data dan memanfaatkan sumber daya jaringan untuk menghalangi akses lainnya [2]. DDoS sendiri merupakan variasi dari serangan DoS (*Denial of Service*) dan Botnet, dengan perbedaan utama terletak pada distribusi sumber serangan. Pada DDoS, jalur serangan berasal dari berbagai sumber, sedangkan DoS hanya mengandalkan satu sumber serangan [3]. Sedangkan Botnet merupakan serangan DDoS yang dipicu oleh ancaman yang menonjol dalam jaringan perangkat yang terkompromi dan dikendalikan oleh penyerang untuk menjalankan aktivitas berbahaya seperti serangan DDoS, distribusi spam, dan pencurian data. Botnet ini, yang dikelola melalui server komando dan kontrol, mengganggu layanan online dan infrastruktur secara mengejutkan [4]. Oleh karena itu Berbagai teknik pendeteksian telah dikembangkan untuk menghadapi serangan DDoS. Ketika serangan DDoS ataupun DoS dilancarkan ke suatu server, maka akan terlihat perilaku Botnet yang secara signifikan mempengaruhi jaringan dan terjadi pada waktu yang hampir bersamaan ini disebut dengan *network behavior*, dengan memanfaatkan lebih banyak sumber serangan, menggabungkan ketiga jenis serangan ini dalam satu sistem akan mempermudah deteksi dan pengendalian ancaman secara keseluruhan terhadap IDS [5].

Dalam bidang keamanan siber, IDS (Intrusion Detection System) adalah elemen penting dari keamanan jaringan yang mengamati dan mengevaluasi lalu lintas pada arsitektur jaringan, ataupun dalam *cloud computing* [6]. IDS bekerja dengan cara memantau aktivitas jaringan secara real-time. Sistem ini mencari pola atau perilaku yang tidak biasa. Melalui data yang dianalisis meliputi alamat IP, port, protokol, waktu akses, dan volume lalu lintas. IDS digunakan untuk mendeteksi aktivitas mencurigakan, pelanggaran kebijakan keamanan, atau akses tidak sah ke sistem jaringan [7]. Beberapa metode pendeteksian yang umum digunakan antara lain adalah berbasis *signature*, deteksi anomali, dan pembelajaran mesin. Sistem IDS berbasis deret waktu juga banyak dikembangkan karena mampu menganalisis pola temporal dan mendeteksi serangan secara berurutan dari waktu [8].

Untuk mendeteksi pola dalam data deret waktu, terdapat berbagai pendekatan seperti *sequence*, *sequence-to-sequence*, dan *sub-sequence.* yang pendekatannya didasarkan pada struktur model RNN, LSTM, CNN, BiLSTM. Pendekatan *sequence* digunakan untuk mengenali pola berurutan, sedangkan *sequence-to-sequence* memetakan urutan input ke output. Agar proses pembelajaran lebih optimal, data diubah menjadi *sub-sequence* pendek menggunakan teknik sliding window, yang menangkap potongan data pada waktu tertentu. Teknik ini berkembang menjadi sliding window *sequence*, dimana setiap jendela input menghasilkan urutan keluaran untuk membantu model mengenali perubahan pola secara lokal [9].

Namun demikian, penerapan deteksi berdasarkan waktu menghadapi tantangan akibat sifat data yang dinamis dan tidak stasioner, sehingga distribusinya cenderung berubah seiring waktu. Tantangan lain muncul dari tingginya dimensi data dan adanya noise yang tidak merata, yang dapat menurunkan kinerja deteksi bila tidak ditangani dengan pendekatan adaptif dan sensitif terhadap perubahan data [10]. Oleh karena itu, pengurutan data dengan teknik sliding window menjadi penting untuk membantu model beradaptasi secara berkelanjutan dan tetap akurat dalam

mendeteksi serangan [11]. Pendekatan ini juga menghasilkan deret waktu yang lebih terstruktur dan siap untuk dianalisis pada model yang dibangun [12].

Penelitian sebelumnya terkait deteksi urutan waktu telah di kaji oleh R. V. Rishika [13] (2025) menunjukkan bahwa kombinasi LSTM dan GRU dengan pendekatan *sequence* berbasis Timestamp (ukuran 10) pada dataset CIC-IDS2018 dan tiga fitur (Dst port, protokol, Timestamp) mampu meningkatkan akurasi deteksi IDS hingga 97,21%. Sementara itu, R. Chinnasamy, M. Subramanian [14] (2025) mengembangkan model hybrid CNN-GRU yang diperkuat GNN dengan pendekatan sliding window pada IoT berbasis IDS dengan dataset ToN-IoT, dan mencapai akurasi hingga 98%.

Penelitian lain terkait perbandingan oleh Q. M. Alzubi [15] (2025) membandingkan algoritma seleksi fitur seperti GWO, BA, dan PIO pada dataset CSE-CIC-IDS2018. GWO terbukti meningkatkan akurasi hampir 99% dengan efisiensi tinggi, dan disarankan untuk dikombinasikan dengan CNN-LSTM pada penelitian mendatang. Di sisi lain perbandingan model oleh, Md. A. Hossain [16] (2025) membandingkan 1D-CNN, LSTM, RNN, dan MLP pada dataset CIC-IoT-DIAD 2024. Hasilnya, 1D-CNN unggul dalam klasifikasi biner (99,53%) dan multi-kelas (99,12%) karena kemampuannya menangkap pola spasial dan temporal.

Penelitian oleh Ziyi Xu [17] (2025) mengusulkan hybrid CNN-LSTM untuk deteksi serangan DDoS pada dataset CICDDoS2019. Model ini memanfaatkan kekuatan CNN dalam ekstraksi fitur spasial dan LSTM untuk pola temporal jangka panjang, dengan akurasi pelatihan 98,75% dan validasi 98,70%. Model berhasil mengenali berbagai jenis serangan seperti NTP, SYN, dan UDP secara efektif.

Berdasarkan penjabaran penelitaian pada [13], [14], [15], [16], [17]. berbagai studi menunjukkan bahwa model hybrid deep learning seperti CNN-GRU dan CNN-LSTM mampu memberikan performa tinggi dalam mendeteksi serangan siber, termasuk serangan DDoS. Pendekatan sliding

window juga umum digunakan untuk merepresentasikan pola waktu dalam data lalu lintas jaringan. Namun, hanya sedikit penelitian yang secara khusus menyoroti deteksi serangan DDoS dengan mempertimbangkan dimensi waktu secara eksplisit. Dalam hal ini, 1D-CNN unggul dalam mengekstraksi fitur spasial dari data sekuensial, sementara LSTM efektif dalam mengenali hubungan temporal jangka panjang. Berdasarkan hal tersebut, penelitian ini mengusulkan judul Deteksi Serangan DDoS pada *Intrusion Detection System* Berdasarkan Waktu dengan Sliding Window Menggunakan Hybrid 1D CNN-LSTM untuk mengenali pola serangan secara lebih tepat dan adaptif terhadap perubahan pola serangan.

1.2 Rumusan Masalah

Berdasarkan penjabaran yang telah diuraikan, maka dirumuskan beberapa rumusan masalah terkait penelitian, diantaranya;

a) Bagaimana hasil akurasi yang dihasilkan dari proses deteksi DDoS menggunakan Hybrid 1D CNN-LSTM?
b) Bagaimana penerapan Sliding Window memberikan dampak terhadap hasil deteksi pada model yang dibangun?

1.3 Tujuan Penelitian

Berdasarkan beberapa rumusan masalah tersebut, maka tujuan pada penelitian ini diantaranya;

a) Menganalisis hasil akurasi Hybrid 1D CNN-LSTM dalam Deteksi serangan DDoS.
b) Mengetahui penerapan Sliding Window terhadap hasil deteksi DDoS pada model yang dibangun.

1.4 Batasan Penelitian

Penelitian ini adalah pengembangan dari penelitian-penelitian yang sudah ada, penelitian ini dilakukan pada dataset yang sudah tersedia pada Kaggle.com. Maka oleh karena itu penelitian ini memberikan batasan agar

peneliti tidak melakukan penyimpangan yang terlalu jauh terhadap judul. Batsan yang disusun sebagai berikut:

a. Penelitian ini hanya menggunakan 5 file dari 10 file, serta menggunakan fitur hasil dari *Feature Selection* dari 80 fitur yang tersedia pada dataset CIC-IDS-2018.
b. Data yang digunakan dalam penelitian ini hanya mencakup serangan jenis Benign, DoS, DDoS dan Bot.
c. Penelitian ini hanya fokus pada hasil Deteksi DDoS dengan Sliding Window menggunakan Hybrid 1D CNN-LSTM.