202110370311338
Satria Milan Wicaksana
Prodi Informatika

BAB II
TINJAUAN PUSTAKA

2.1 Studi Literatur

Studi literatur pada penelitian ini memuat beberapa penelitian dan metode yang dapat mendukung penelitian ini. Dibawah ini merupakan penelitian terdahulu dapat dilihat pada Table 2. 1.

Tabel 2. 1. Penelitian Terdahulu dan Pendukung.

No	Penulis (Tahun)	Judul	Dataset	Metode	Hasil Pembahasan
1	R. V. Rishika (2025)	Network Intrusion Detection System with Time-Based Sequential Cluster Models Using LSTM and GRU	CIC-IDS-2018	LSTM, GRU	Pengelompokan data secara berurutan berdasarkan waktu (*sequence size* 10) dengan hanya 3 fitur utama (Dst port, Protocol, Timestamp) berhasil meningkatkan akurasi deteksi hingga 97,21%.
2	R. Chinnasamy, M. Subramanian (2025)	Contextual Internet of ThingsIntrusion Detection: A Sliding Window Convolutional Neural Network–Gated Recurrent Unit	ToN-IoT	hybrid 1D-CNN-GRU-GNN	Model hybrid CNN-GRU diperkuat GNN dengan sliding window size 10 mampu menangkap fitur spasial, temporal, dan hubungan antar node IoT. Evaluasi pada dataset ToN-IoT menunjukkan akurasi

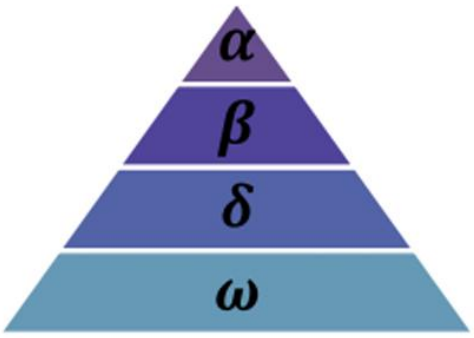
		Model Enhanced by Graph Neural Networks			98% dan AUC 1.00. Efektif untuk deteksi intrusi kontekstual di lingkungan IoT.
3	Q. M. Alzubi (2025)	Optimizing Intrusion Detection: Advanced Feature Selection and Machine Learning Techniques Using the CSE-CIC-IDS2018 Dataset	CSE-CIC-IDS2018	GWO, BA, PIO (*feature selection*)	menurunkan fitur dari 80 menjadi 10, 6, dan 7 tanpa mengorbankan akurasi. Akurasi hampir mencapai 99%. Disarankan pengembangan model hybrid CNN-LSTM untuk penelitian ke depan.
4	Md. A. Hossain (2025)	Deep Learning-Based Intrusion Detection for IoT Networks: A Scalable and Efficient Approach	CIC IoT-DIAD 2024	1D-CNN, LSTM, RNN, MLP	Evaluasi performa empat arsitektur deep learning untuk klasifikasi biner dan multi-kelas. 1D-CNN unggul dengan akurasi 99,12% (multi-kelas) dan 99,53% (biner). LSTM, RNN, dan MLP mengikuti dengan akurasi >97%. 1D-CNN unggul dalam menangkap pola spasial dan temporal

5	Ziyi Xu (2025)	Deep Learning Based DDoS Attack Detection	CIC DDoS 2019	hybrid CNN-LSTM	Model hybrid CNN-LSTM Dimana memanfaatkan kekuatan 1D-CNN dalam mengekstraksi fitur spasial dari urutan data jaringan serta LSTM dalam menangkap pola temporal jangka Panjang, menggabungkan fitur spasial dan temporal. Akurasi pelatihan 98.75% dan validasi 98.70%, F1-score mendekati 1.00 untuk serangan deteksi berbagai jenis serangan DDoS.

2.2 Feature Selection

Feature Selection merupakan langkah dari preprocessing dengan tujuan untuk mengidentifikasi fitur yang paling optimal dalam suatu dataset dengan menghilangkan data yang redundan sambil mempertahankan akurasi klasifikasi setinggi mungkin [18]. Dengan pendekatan *Grey Wolf Optimizer* (GWO) yang terinspirasi oleh perilaku berburu kawanan serigala mengakui hierarki sosial yang berbeda dalam kelompok serigala, mengelompokkan serigala ke dalam empat kategori yang mencerminkan status hierarkis mereka. Di puncak hierarki ini adalah serigala Alpha(α), Beta(β), Delta(δ), dan Omega(ω). Proses ini dapat ditangkap melalui

kerangka matematis dimana posisi serigala disesuaikan berdasarkan lokasi mangsanya untuk memperbarui posisi serigala diiterasi berikutnya [19].



Gambar 2. 1. The social structure of GWO [15].

Dalam GWO, proses pembaruan posisi agen (solusi sementara) tidak dilakukan secara acak, melainkan berdasarkan pendekatan terarah terhadap posisi tiga individu terbaik dalam populasi, yaitu serigala Alpha (α), Beta (β), dan Delta (δ). Ketiga serigala ini dianggap mewakili solusi terbaik yang pernah ditemukan selama iterasi berlangsung. Posisi dari setiap serigala lain akan diperbarui dengan mempertimbangkan pengaruh dari ketiga pemimpin tersebut menggunakan mekanisme matematis tertentu yang mengatur jarak, arah, serta probabilitas eksplorasi dan eksploitasi dalam pencarian solusi optimal. Persamaan matematis yang

merepresentasikan pembaruan posisi ini dapat dilihat pada pendekatan dan penejelasan tertera oleh Q. M. Alzubi [15], sebagai berikut:

$$a = 2\left(1 - \frac{t}{T}\right) \quad (1)$$

Parameter a mengontrol keseimbangan antara eksplorasi dan eksploitasi. Parameter ini menurun secara linear dari 2 ke 0 seiring dengan bertambahnya jumlah iterasi t mendekati jumlah iterasi maksimum T [15].

$$A = 2ar_1 - a, C = 2r_2 \quad (2)$$

A adalah parameter yang digunakan untuk mengontrol dampak posisi serigala selama fase berburu. Nilainya dipengaruhi oleh a dan r_1, dimana a adalah angka acak yang terdistribusi antara 0 dan 1. C adalah parameter lain yang memperkenalkan unsur kebetulan ke dalam proses pencarian melalui r_2, angka acak lain yang juga terdistribusi uniform antara 0 dan 1 [15].

$$D = \left|CX_p(t) - X(t)\right| \quad (3)$$

D mewakili jarak antara posisi serigala saat ini $X(t)$ dan posisi mangsa $X_p(t)$, yang diperkirakan berdasarkan posisi serigala alpha, beta,

dan delta. C menambahkan elemen acak pada perhitungan jarak, membantu menghindari konvergensi yang terlalu cepat [15].

$$X(t+1) = X_p(t) + A.D \tag{4}$$

Persamaan ini memperbarui posisi serigala berdasarkan posisi saat ini dan jarak yang diperkirakan dari mangsa [15].

2.3 Sliding Window

Sliding window merupakan teknik pembentukan struktur pada data rangkaian waktu [9]. Dengan cara membagi data menjadi segmen-segmen *Sequence*. Metode ini bertujuan untuk menangkap dinamika temporal dalam data dengan lebih baik, sehingga model dapat mengenali pola berurutan secara lebih akurat. Penjelasan dari Sliding window tertera pada penelitian R. Chinnasamy, M. Subramanian [14], sebagai berikut:

$$X_i = [x_i, x_{i+1}, x_{i+2}, \ldots, x_{i+T-1}] \in \mathbb{R}^{T \times d} \text{ dan } \mathcal{Y}_i = \mathcal{Y}_{i+T-1} \tag{5}$$

Keterangan:

X_i = Merupakan inputan *sequence*.

T = Ukuran sliding window.

d = Dimensi fitur.

$\mathcal{Y}_i$ = Label dari Timesatamp.

2.4 *1D Convolutional Neural Network* (1D CNN)

1D Convolutional Neural Network (1D CNN) merupakan arsitektur deep learning yang masih terdapat pada CNN tetapi dalam ranah konvolusi 1 dimensi yang dirancang khusus untuk memproses data sekuensial satu dimensi seperti sinyal waktu atau lalu lintas jaringan, serta banyak

digunakan dalam berbagai aplikasi seperti klasifikasi, deteksi anomali, dan sistem keamanan siber. Selain itu, terdapat *Activation functions Rectified Linear Unit* (ReLU), dan Sigmoid (σ) yang diterapkan pada *hidden layer* [20]. Serta dalam mengekstraksi fitur spasial dari input sekuensial melalui operasi konvolusi, dimana kernel bergerak sepanjang data input untuk menangkap pola yang bermakna, Penjelasan dari 1D CNN tertera pada penelitian R. Chinnasamy, M. Subramanian [14], sebagai berikut:

$$h_j = \sigma\left(\sum_{k=0}^{K-1} \omega_k \cdot x_{j+k} + b\right), j = 1,2,3,\ldots,T-K+1 \quad (6)$$

Keterangan:

ω_k = Merupakan berat kernel.

K = Ukuran kernel.

b = Nilai bias.

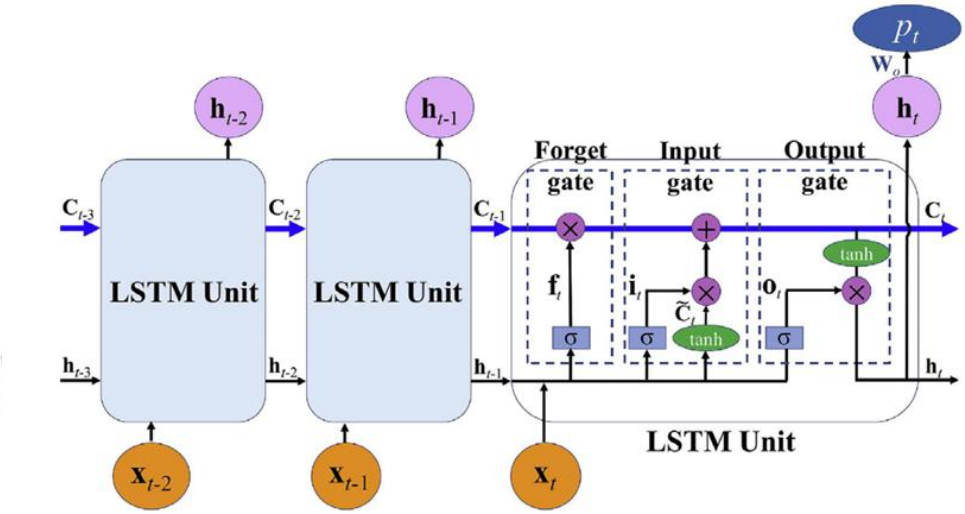
σ = *Activation functions* Sigmoid.

h_j = Mempresentaikan hasil konvolusi pada posisi ke- j.

2.5 *Long Short-Term Memory* (LSTM)

Long Short-Term Memory (LSTM) dirancang untuk mengatasi pemrosesan data sekuensial, serta memiliki kemampuan untuk menyimpan informasi dalam jangka waktu panjang. LSTM terdiri dari tiga *gate*/gerbang utama yaitu *forget gate*, *input gate*, dan *output gate* yang dimana tiap *gate*/gerbang tersebut berfungsi untuk mengatur informasi yang disimpan atau dihapus dalam sel memori[21]. Selain itu, terdapat *Activation functions Hyperbolic Tangent Function* (Tanh), dan Sigmoid (σ) yang merupakan bagian integral dari LSTM, jaringan saraf tiruan yang dirancang khusus untuk menganalisis dan memahami hubungan jangka panjang dalam data melalui metode *deep learning* [22]. Keunggulan utama LSTM adalah kemampuannya dalam menangani dependensi temporal pada data deret

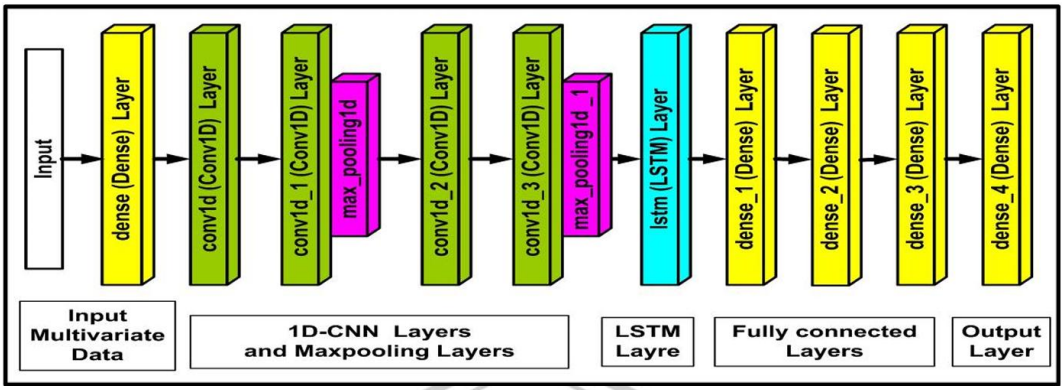
waktu, menjadikannya sangat berguna untuk aplikasi seperti prediksi, analisis sentimen, dan deteksi. Dalam konteks deteksi pada data, LSTM mampu mempelajari pola normal dan mengidentifikasi outlier, baik yang bersifat kontekstual maupun inovatif, yang menyimpang dari pola yang ada. Berikut adalah gambar arsitektur LSTM [23].



Gambar 2. 2 LSTM *Architecture* [23].

2.6 Model Hybrid

Dalam Model Hybrid ini, blok CNN yang merupakan lapisan konvolusi 1D dan lapisan *Max pooling* bertanggung jawab untuk ekstraksi dan pemilihan fitur. Sementara lapisan LSTM yang diberi umpan dengan fitur-fitur ini sebagai fitur yang bergantung pada waktu akan belajar bagaimana mengekstrak informasi kontekstual dari waktu [24]. Dengan membangun model arsitektur hybrid seperti pada Gambar 2. 3.



Gambar 2. 3. The MLIDS22 Model Architecture [25].

Pada Gambar 2.3 menunjukkan arsitektur model hybrid MLIDS22 yang dirancang untuk mendeteksi serangan dalam data multivariat dengan menggabungkan kekuatan 1D-CNN dan LSTM. Proses dimulai dari sebuah lapisan dense awal yang memiliki 256 neuron dengan fungsi aktivasi ReLU, yang berfungsi sebagai tahap ekstraksi awal fitur. Kemudian, data diproses melalui tiga lapisan Conv1D secara berurutan dengan jumlah filter masing-masing 64, 128, dan 256, menggunakan kernel berukuran 3 dan stride 1, semuanya diaktifkan dengan ReLU. Untuk mengurangi dimensi dan mempercepat proses komputasi, operasi max pooling disisipkan setelah lapisan Conv1D pertama dan ketiga. Hasil ekstraksi fitur spasial dari CNN ini kemudian diteruskan ke lapisan LSTM dengan 128-unit yang menggunakan aktivasi tanh, bertugas menangkap hubungan temporal dalam data. Selanjutnya, keluaran dari LSTM dialirkan ke empat lapisan dense bertingkat (128, 64, 32, dan output), dengan softmax sebagai aktivasi akhir untuk melakukan klasifikasi. Setelah itu, pada seluruh model dilatih menggunakan algoritma optimasi Adam dengan learning rate 0.001, fungsi loss categorical crossentropy, batch size sebesar 64, dan selama 10 epoch [25].