JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727

Evaluasi Kinerja CNN, LSTM, dan DNN untuk Deteksi Serangan DDoS Berbasis Flow features pada Dataset CSE-CIC-IDS2018

Muhammad Al Adib[1*], Pebruarianto Hutabarat[2], Heru Fredi[3], Bill Raj[4], Prasetyo[5], Empiter Gea[6]

[1,2,3,4,5,6] Fakultas Teknik Dan Ilmu Komputer , Program Studi Ilmu Komputer, Universitas Potensi Utama, Medan, Indonesia
Email: [1*]dibsowden@gmail.com, [2] rinto@hutabarat.com, [3]herufredi85@gmail.com, [4]denilsdu10@gmail.com, [5]dundarsihite@gmail.com, [6]empitergea07@gmail.com
(* Email Corresponding Author: dibsowden@gmail.com)
Received: 13 Desember 2025 | Revision: 18 Desember 2025 | Accepted: 18 Desember 2025

Abstrak

Pendekatan *deep learning* telah terbukti efektif dalam mendeteksi serangan *Distributed Denial of Service* (DDoS) pada jaringan, terutama melalui analisis *flow features*. Tujuan penelitian ini adalah mengevaluasi CNN, LSTM, dan DNN dalam mendeteksi serangan *DDoS* menggunakan *flow features* pada dataset CSE-CIC-IDS2018. Penelitian ini menggunakan dataset CSE-CIC-IDS2018 untuk mengevaluasi performa CNN, LSTM, dan DNN dalam mendeteksi serangan DDoS berdasarkan *flow features*. Setiap model dibandingkan secara sistematis dengan algoritma *baseline* untuk menilai akurasi, presisi, recall, dan F1-score, sehingga diperoleh model paling optimal bagi *Network Intrusion Detection System* (NIDS). Semua model menunjukkan akurasi sangat tinggi di atas 99%, dengan CNN menonjol sebagai model *deep learning* terbaik untuk mendeteksi pola DDoS, sementara XGBoost m enjadi baseline paling unggul. Hasil ini menegaskan bahwa pemilihan model deteksi harus mempertimbangkan karakteristik data, kompleksitas *flow features*, dan variasi jenis serangan untuk mencapai performa optimal dalam Network Intrusion Detection System (NIDS). Penelitian ini menunjukkan bahwa baik CNN, DNN, dan LSTM maupun baseline seperti XGBoost mampu mendeteksi serangan *DDoS* berbasis *flow features* dengan akurasi di atas 99%, menegaskan efektivitas pendekatan ini dan pentingnya pemilihan model sesuai karakteristik data.

Kata Kunci: *Deep learning*, DDoS Detection, CNN, LSTM, *Flow features*

Abstract

Deep learning approaches have been proven effective in detecting Distributed Denial of Service (DDoS) attacks on networks, particularly through the analysis of flow features. This study aims to evaluate CNN, LSTM, and DNN in detecting DDoS attacks using flow features on the CSE-CIC-IDS2018 dataset. Each model is systematically compared with baseline algorithms to assess accuracy, precision, recall, and F1-score, in order to determine the most optimal model for a Network Intrusion Detection System (NIDS). All models demonstrated very high accuracy above 99%, with CNN standing out as the best-performing deep learning model for detecting DDoS patterns, while XGBoost emerged as the most effective baseline. These results emphasize that the choice of detection model should consider data characteristics, the complexity of flow features, and the diversity of attack types to achieve optimal performance in a NIDS. The study shows that both CNN, DNN, and LSTM, as well as baseline models such as XGBoost, can detect DDoS attacks based on flow features with accuracy above 99%, confirming the effectiveness of this approach and the importance of selecting models according to data characteristics.

Keywords*: Deep learning, DDoS Detection, CNN, LSTM, Flow features*

1. PENDAHULUAN

Dalam beberapa tahun terakhir, pendekatan *deep learning* telah menjadi arus utama dalam penelitian sistem deteksi intrusi jaringan (IDS), sebagai upaya mengatasi keterbatasan metode tradisional yang berbasis tanda tangan. Studi komprehensif menunjukkan bahwa *deep learning* mampu secara otomatis mengekstrak pola kompleks dari trafik jaringan dan menawarkan tingkat deteksi yang lebih tinggi dibanding pendekatan konvensional [1]. Dalam konteks ini, pendekatan berbasis *deep learning* menjadi salah satu arah penelitian yang paling berkembang. Model-model *deep learning* mampu mempelajari representasi fitur secara otomatis dari data trafik jaringan dan mengenali pola yang tidak dapat diidentifikasi melalui teknik konvensional. Penelitian mutakhir menunjukkan bahwa arsitektur seperti *Convolutional Neural Network* (CNN) dan *Long Short-Term Memory* (LSTM) memiliki performa unggul dalam menangkap pola spasial maupun temporal pada data jaringan yang dinamis[2]. Selain itu, tinjauan literatur terkini menegaskan bahwa kebutuhan akan metode deteksi yang adaptif semakin mendesak karena meningkatnya variasi serangan, volume trafik, dan karakteristik anomali trafik yang semakin kompleks [3]. Salah satu ancaman yang paling menonjol dalam lanskap keamanan siber modern adalah *Distributed Denial of Service* (DDoS). Serangan ini bertujuan membanjiri sumber daya layanan dengan trafik masif sehingga layanan tidak dapat diakses oleh pengguna yang sah. Penelitian menunjukkan bahwa frekuensi dan dampak serangan DDoS meningkat secara signifikan, menyebabkan gangguan layanan, kerugian finansial, dan menurunnya kepercayaan pengguna [2], [4], [5], [6]. Kompleksitas varian serangan modern seperti UDP Flood, SYN Flood, HTTP Flood, serta serangan multi-vektor semakin mempertegas perlunya sistem deteksi yang mampu beradaptasi terhadap pola serangan yang dinamis [7].

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727

Sejalan dengan tantangan tersebut, metode *machine learning* dan *deep learning* semakin diadopsi karena kemampuannya dalam menangani data berdimensi besar, mempelajari pola non-linear, dan beradaptasi terhadap perubahan perilaku trafik. *Deep Neural Network* (DNN) efektif dalam mempelajari fitur statis, CNN unggul dalam mengekstraksi pola spasial, sedangkan LSTM memiliki keunggulan dalam mengenali dinamika temporal aliran trafik [8]. Ketiga arsitektur ini telah banyak diterapkan pada penelitian *Network Intrusion Detection System* (NIDS), namun hasil evaluasinya menunjukkan variasi performa yang berbeda tergantung jenis serangan dan karakteristik data. Dalam penelitian berbasis *flow features*, dataset CSE-CIC-IDS 2018 menjadi salah satu dataset yang paling banyak digunakan karena mencakup skenario serangan yang realistis, termasuk berbagai bentuk serangan DDoS, serta menyediakan lebih dari 80 *flow features* yang relevan untuk analisis trafik jaringan [9]. Ketersediaan fitur yang beragam dan representatif ini menjadikan dataset tersebut ideal untuk pengembangan dan evaluasi model *deep learning* berbasis *flow-level detection*. Meskipun penelitian terkait deteksi intrusi berbasis *deep learning* terus berkembang, terdapat beberapa celah penelitian yang masih belum banyak dibahas. Studi mengenai deteksi DDoS berbasis *flow features* masih terbatas, terutama yang melakukan komparasi langsung antara CNN, LSTM, dan DNN dengan menggunakan dataset yang sama. Literatur sebelumnya juga menunjukkan belum adanya standar metrik evaluasi yang konsisten serta minimnya analisis mengenai stabilitas, efisiensi, dan akurasi antar model [10]. Oleh karena itu, evaluasi komprehensif terhadap ketiga arsitektur *deep learning* pada skenario serangan DDoS modern menjadi sangat diperlukan.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan mengevaluasi performa tiga arsitektur *deep learning Convolutional Neural Network* (CNN), *Long Short-Term Memory* (LSTM), dan *Deep Neural Network* (DNN) dalam mendeteksi serangan DDoS menggunakan *flow features* pada dataset CSE-CIC-IDS 2018. Evaluasi dilakukan menggunakan metrik akurasi, presisi, recall, dan *F1-score* untuk menentukan model yang paling optimal dalam mendukung pengembangan *Network Intrusion Detection System* (NIDS) berbasis *deep learning*. Penelitian ini diharapkan dapat memberikan kontribusi ilmiah dalam bentuk analisis perbandingan yang sistematis dan terukur terhadap tiga arsitektur *deep learning* yang paling umum digunakan dalam deteksi intrusi jaringan. Dengan menggunakan dataset dan skenario evaluasi yang sama, hasil penelitian ini diharapkan mampu memberikan gambaran yang lebih objektif mengenai kelebihan dan keterbatasan masing-masing model dalam mendeteksi serangan *Distributed Denial of Service* (DDoS) berbasis *flow features*. Selain itu, analisis performa yang komprehensif diharapkan dapat mengurangi bias evaluasi yang sering muncul akibat perbedaan konfigurasi data dan lingkungan pengujian pada penelitian sebelumnya. Lebih lanjut, penelitian ini juga mempertimbangkan aspek efisiensi dan stabilitas model sebagai faktor pendukung dalam implementasi sistem *Network Intrusion Detection System* (NIDS) di lingkungan nyata. Dalam konteks operasional, sistem deteksi intrusi tidak hanya dituntut memiliki tingkat akurasi yang tinggi, tetapi juga harus mampu bekerja secara efisien dengan latensi rendah serta adaptif terhadap perubahan pola trafik jaringan. Oleh karena itu, pemahaman terhadap karakteristik masing-masing arsitektur *deep learning* menjadi penting dalam menentukan model yang paling sesuai untuk diterapkan pada skenario jaringan berskala besar dan dinamis. Hasil penelitian ini diharapkan dapat menjadi referensi bagi peneliti dan praktisi keamanan siber dalam memilih dan mengembangkan model *deep learning* yang optimal untuk deteksi serangan DDoS. Selain itu, temuan penelitian ini juga berpotensi membuka peluang penelitian lanjutan, seperti pengembangan model *hybrid*, penerapan teknik *ensemble learning*, serta eksplorasi metode optimasi dan *feature selection* untuk meningkatkan performa deteksi. Dengan demikian, penelitian ini tidak hanya berkontribusi pada pengembangan keilmuan di bidang keamanan jaringan, tetapi juga mendukung upaya peningkatan ketahanan infrastruktur jaringan terhadap ancaman siber modern.

2. METODOLOGI PENELITIAN

2.1 Jenis dan Pendekatan Penelitian

Penelitian ini bersifat kuantitatif dengan pendekatan *experimental research*, menilai performa arsitektur *deep learning* (DNN, CNN, LSTM) dalam mendeteksi serangan *Distributed Denial of Service* (DDoS) menggunakan dataset CSE-CIC-IDS2018, dengan seluruh model diuji pada dataset yang sama melalui tahapan pengumpulan data, praproses, pengembangan, dan evaluasi berbasis metrik klasifikasi untuk memastikan perbandingan objektif.

2.2 Metode Pengumpulan Data

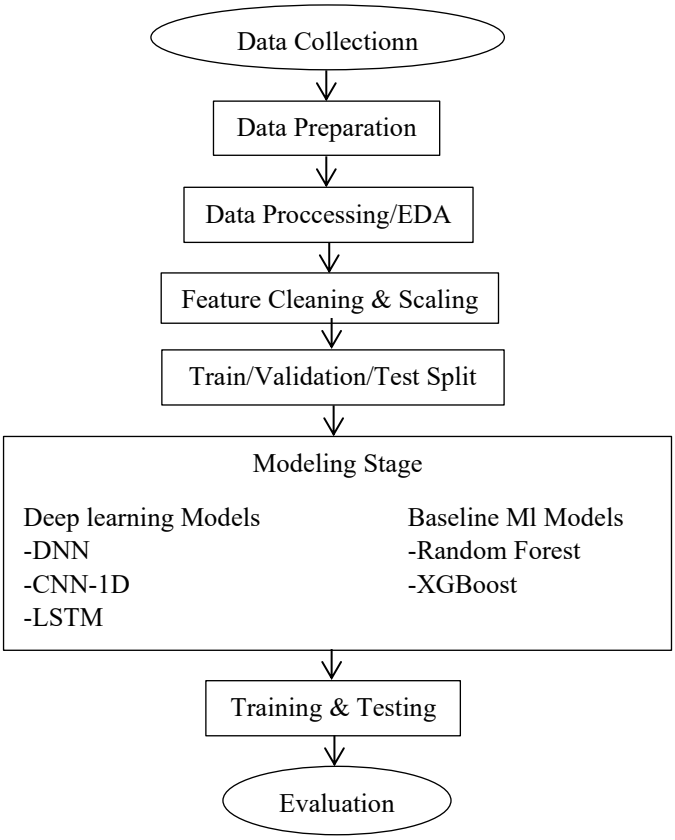
Data penelitian ini diperoleh dari dataset CSE-CIC-IDS2018, yaitu dataset intrusi jaringan yang berisi trafik normal dan beberapa kategori serangan, seperti serangan DoS/DDoS, *brute-force, botnet, web attacks*, dan infiltrasi jaringan. Dataset ini dikumpulkan dalam lingkungan jaringan nyata dan menyediakan fitur aliran jaringan (*flow features*) yang kaya sehingga cocok untuk penelitian deteksi intrusi berbasis *machine learning* dan *deep learning* [11]. Seluruh data diunduh dari repositori resmi CIC dalam format *Parquet* yang efisien untuk data berukuran besar, kemudian digabungkan menjadi

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727

satu dataset untuk mencakup seluruh skenario serangan. Proses pengumpulan dilakukan sepenuhnya dari sumber publik tanpa perekaman manual, sehingga penelitian mudah direplikasi.

2.3 Model Development

Tahap pengembangan model (*model development*) meliputi pemilihan fitur dan algoritma, penyetelan parameter, serta validasi untuk mencapai performa deteksi *Distributed Denial of Service (DDoS)* yang optimal, sebagaimana ditunjukkan pada diagram alir berikut.



Gambar 1. Model Development

Untuk mendukung proses pengembangan model tersebut, penelitian ini dilakukan melalui beberapa tahapan utama yang disusun secara berurutan, mulai dari pengumpulan data hingga evaluasi kinerja model, sebagaimana dijabarkan berikut ini:

a. Data *Collection* : Mengumpulkan dataset CSE-CIC-IDS2018 sebagai sumber utama untuk eksperimen deteksi serangan DDoS.
b. Data *Preparation* : Melakukan persiapan awal data seperti penggabungan file, pengecekan kelengkapan, dan penanganan nilai kosong.
c. Data *Processing* / EDA : Mengeksplorasi struktur dan distribusi data untuk memahami pola trafik dan karakteristik serangan.
d. *Feature Cleaning & Scaling* : Membersihkan fitur yang tidak relevan, mengatasi inkonsistensi, dan melakukan scaling pada data numerik agar siap untuk pelatihan model.
e. *Train / Validation / Test Split* : Membagi dataset menjadi bagian pelatihan, validasi, dan pengujian untuk memastikan model mampu melakukan generalisasi.
f. Modeling Stage : Tahap pemodelan dilakukan pada dua kelompok model.
   1. *Deep learning*: DNN, CNN-1D, dan LSTM.
   2. Baseline *Machine learning*: Random Forest dan XGBoost sebagai pembanding performa.
g. *Training & Testing* : Melatih setiap model menggunakan train set, kemudian menguji performanya pada test set.
h. *Evaluation* : Mengukur kinerja model menggunakan metrik seperti Accuracy, Precision, Recall, F1-score, *Confusion matrix*, serta analisis per jenis serangan.

2.4 Evaluasi Kinerja Model

Evaluasi kinerja model dilakukan untuk menilai kemampuan model dalam mendeteksi serangan DDoS berbasis *flow features*. Pada penelitian ini, performa model diukur menggunakan beberapa metrik klasifikasi, yaitu *accuracy*, *precision*,

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727

recall, dan *F1-score*. Metrik tersebut dipilih karena mampu memberikan gambaran yang komprehensif terhadap tingkat ketepatan klasifikasi model pada data tidak seimbang.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F1 - Score = 2\ x\ \frac{Precision\ x\ Recall}{Precision+Recall} \quad (4)$$

3. HASIL DAN PEMBAHASAN

3.1 Data Collection

Penelitian ini menggunakan dataset CSE-CIC-IDS2018 sebagai sumber utama untuk eksperimen deteksi DDoS, terdiri dari dua file:

a. DDoS1-Tuesday-20-02-2018_TrafficForML_CICFlowMeter.parquet
b. DDoS2-Wednesday-21-02-2018_TrafficForML_CICFlowMeter.parquet

Dataset ini mencakup flow-level features dari trafik jaringan benign dan serangan DDoS, memungkinkan model belajar pola serangan yang bervariasi dan representatif. Format Parquet memudahkan pemrosesan dan mendukung penggunaan langsung pada *machine learning* dan *deep learning*.

3.2 Data Preparation

Tahap ini bertujuan menyiapkan dataset untuk proses pemodelan dengan menggabungkan dua file parquet (*DDoS1-Tuesday-20-02-2018* dan *DDoS2-Wednesday-21-02-2018*). Seluruh kolom numerik digunakan sebagai fitur, sementara kolom konstan dihapus karena tidak informatif. Nilai kosong (*NaN*) diisi menggunakan median, dan kolom *Label* digunakan sebagai target klasifikasi untuk skenario *binary* maupun *multi-class*.

Tabel 1. Data Preparation

Idle Mean	Idle Std	Idle Max	Idle Min	Label
0.0	0.000000	0	0	Benign
56,300,000.0	7.071068	56,300,000	56,300,000	Benign
56,300,000.0	18.384777	56,300,000	56,300,000	Benign
56,300,000.0	5.656854	56,300,000	56,300,000	Benign
56,300,000.0	65.053825	56,300,000	56,300,000	Benign

Tahap ini memastikan dataset bersih, konsisten, dan siap untuk tahap selanjutnya, yaitu EDA dan *feature scaling*, sehingga mencegah bias dan mendukung performa model yang optimal.

3.3 Data Processing / EDA

Tahap *EDA* dilakukan untuk memahami struktur dataset sebelum pemodelan. Dataset terdiri dari 78 fitur numerik dan 1 kolom *Label* sebagai target klasifikasi, dengan hasil pemeriksaan menunjukkan tidak adanya *missing value* yang signifikan.

Tabel 2. Struktur Dataset CSE-CIC-IDS2018

No	Fitur	Tipe Data	Deskripsi Singkat
1	Protocol	int8	Protokol jaringan (TCP, UDP, dll.)
2	Flow Duration	int32	Durasi flow (dalam microseconds)
3	Total Fwd Packets	int32	Total paket forward
4	Total Backward Packets	int16	Total paket backward
5	Fwd Packet Length Mean	float32	Rata-rata panjang paket forward
6	Bwd Packet Length Mean	float32	Rata-rata panjang paket backward
7	Label	object	Target klasifikasi (Benign/DDoS)

Distribusi label menunjukkan imbalance kelas, dengan mayoritas sample berasal dari kelas Benign dan DDoS attacks-LOIC-HTTP. Hal ini menekankan perlunya penanganan imbalance saat *training*, misalnya menggunakan SMOTE pada *training set*. Informasi EDA ini menjadi dasar untuk tahap *feature cleaning, scaling*, dan *split* data selanjutnya.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727

Tabel 3. Distribusi Label Dataset

Kelas	Jumlah Sample
Benign	740,287
DDoS attacks-LOIC-HTTP	575,364
DDOS attack-HOIC	198,861
DDOS attack-LOIC-UDP	1,730

3.4 Feature Cleaning & Scaling

Pada tahap persiapan fitur, kolom non-numerik dan fitur konstan dihapus sehingga tersisa 70 fitur numerik. Seluruh fitur kemudian distandarisasi menggunakan *StandardScaler* dan dibagi ke dalam data *train-validation-test* untuk mendukung proses pemodelan yang stabil dan optimal.

3.5 Train / Validation / Test Split

Dataset yang telah dibersihkan dan distandarisasi dibagi menjadi *training* (1,061,369 sample, 70%), *validation* (227,436 sample, 15%), dan test (227,437 sample, 15%) secara stratified. Sebelum SMOTE, distribusi kelas pada *training* set tidak seimbang, terutama kelas minoritas DDOS attack-LOIC-UDP. Setelah SMOTE, semua kelas diseimbangkan menjadi 518,201 sample per kelas, sehingga model DNN, CNN-1D, LSTM, dan baseline ML dapat belajar secara adil dan meningkatkan generalisasi.

3.6 Modeling Stage

Tahap pemodelan dilakukan dengan membangun tiga arsitektur *deep learning* DNN, CNN 1D, dan LSTM serta dua model *machine learning* baseline, yaitu Random Forest dan XGBoost. Tujuan tahap ini adalah mengembangkan model yang mampu mempelajari pola trafik normal dan DDoS berdasarkan *flow features* dari dataset CSE-CIC-IDS2018.

a. Deep learning Models

Model *deep learning* dirancang dengan konfigurasi sebagai berikut:

1. DNN menggunakan dua hidden layer beraktivasi ReLU dengan dropout untuk mencegah overfitting.
2. CNN 1D terdiri dari dua lapisan convolution untuk mengekstraksi pola lokal antar fitur, diikuti flatten dan dense layer.
3. LSTM menggunakan dua lapisan LSTM bertingkat untuk menangkap dependensi temporal dalam data flow.

Tabel 4. Hyperparameter Model Deep learning

Model	Arsitektur / Layer	Activation	Optimizer	Loss Function	Keterangan
DNN	Dense 128 → Dense 64 + Dropout	ReLU	Adam	Sparse CCE	Dropout 0.3 tiap layer
CNN 1D	Conv1D 64 → Conv1D 32 → Flatten	ReLU	Adam	Sparse CCE	Kernel size 3
LSTM	LSTM 64 → LSTM 32 → Dense 32	ReLU	Adam	Sparse CCE	return_sequences pada layer pertama

b. Baseline Machine learning Models

Dua algoritma *machine learning* digunakan sebagai baseline untuk membandingkan performa *deep learning* pada dataset yang sama.

1. Random Forest menggunakan 200 pohon keputusan dengan kedalaman maksimum 20.
2. XGBoost dibangun dengan 200 estimators, learning rate 0.05, dan max depth 8.

Tabel 5. Hyperparameter Model *Machine* learning

Model	Hyperparameter Utama
Random Forest	n_estimators=200, max_depth=20, n_jobs=-1
XGBoost	n_estimators=200, learning_rate=0.05, max_depth=8, subsample=0.8, colsample_bytree=0.8

3.7 Training & Testing

Pada tahap ini, setiap model dilatih menggunakan dataset CSE-CIC-IDS2018 yang telah dibagi menjadi 70% *training*, 15% *validation*, dan 15% *testing*. Seluruh fitur telah dinormalisasi, dan label disesuaikan dengan kebutuhan masing-masing arsitektur. Proses pelatihan menggunakan optimizer Adam dan loss function cross-entropy. Early stopping diterapkan berdasarkan performa *validation* set untuk menghindari overfitting. Setelah pelatihan selesai, model dievaluasi

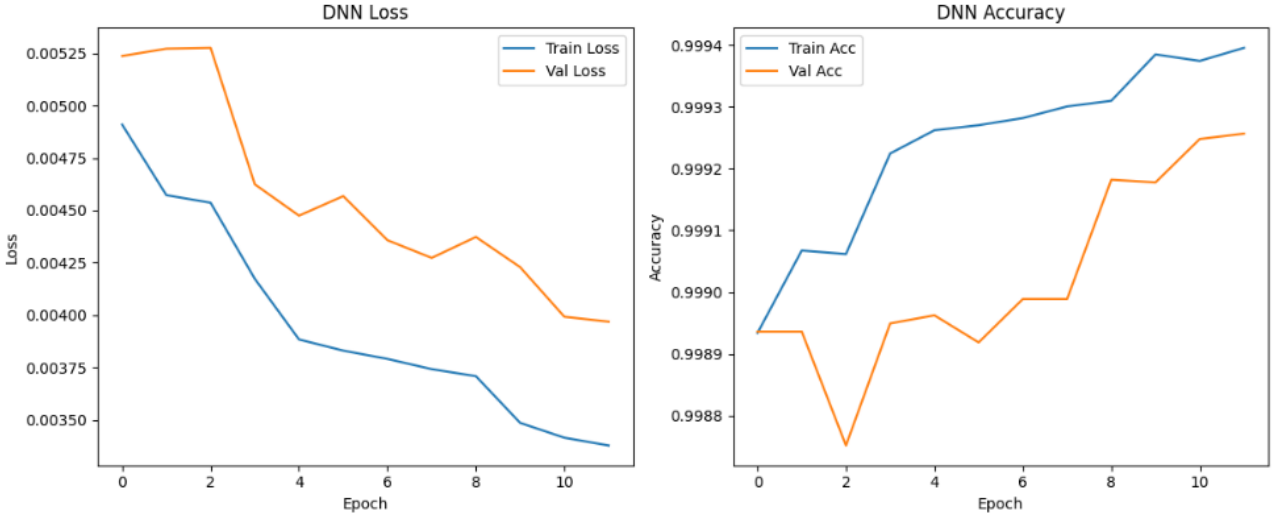
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727

menggunakan test set untuk memperoleh metrik performa seperti accuracy, precision, recall, F1-score, serta *confusion matrix*.

a. Model Deep learning

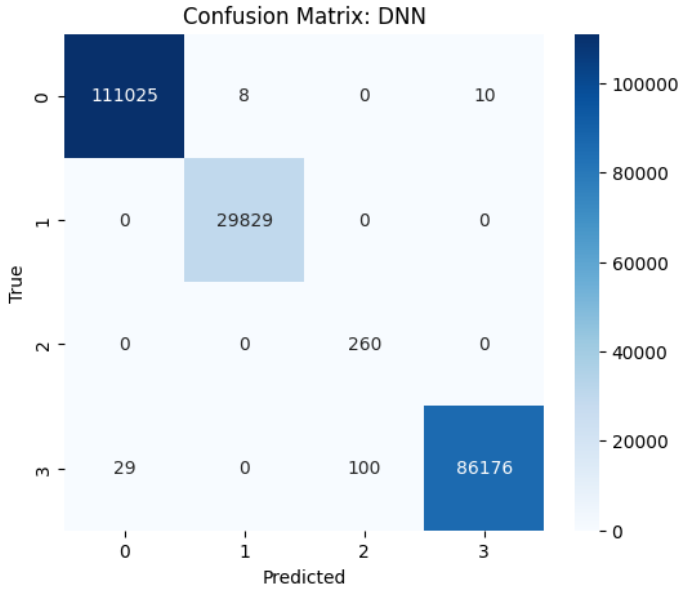
1. Deep Neural Network (DNN)

DNN adalah algoritma *deep learning* berbasis jaringan saraf yang digunakan untuk pengambilan keputusan. Algoritma ini memiliki struktur berlapis yang meniru jaringan saraf manusia dan hewan untuk mengenali pola, yang dikenal sebagai *neural network* (NN) [12]. DNN digunakan sebagai salah satu arsitektur *deep learning* berbasis lapisan fully-connected untuk mempelajari hubungan non-linear antar *flow features*.



Gambar 2. Plot Kurva Pelatihan Model DNN

Kurva pelatihan menunjukkan penurunan loss yang konsisten serta akurasi yang stabil pada train dan *validation*, menandakan proses pembelajaran yang baik.



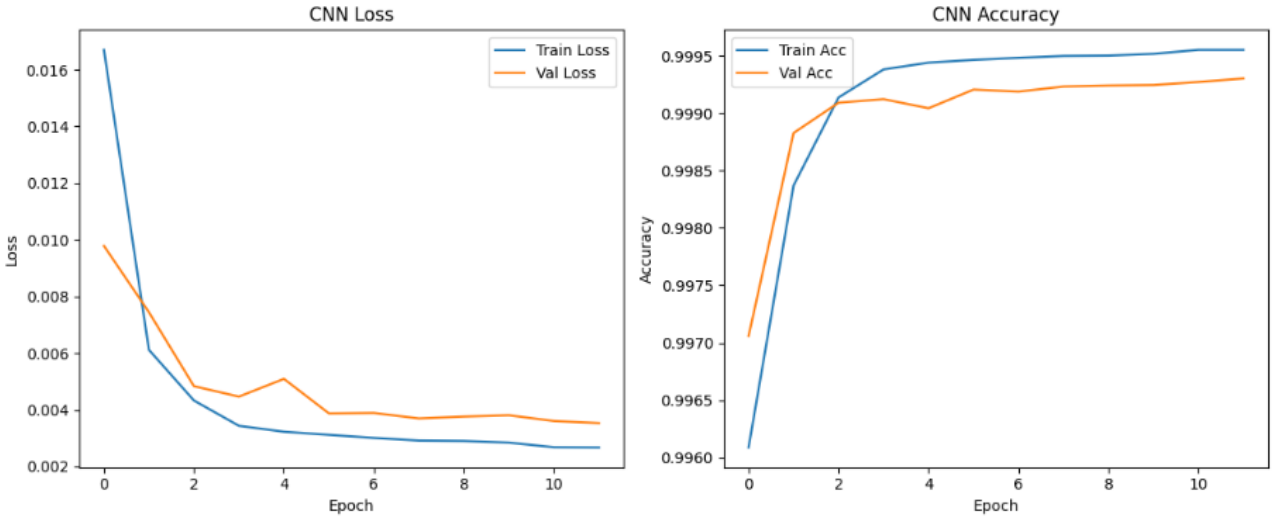
Gambar 3. *Confusion matrix* Model DNN

Confusion matrix menunjukkan bahwa DNN mampu mengklasifikasikan trafik normal dan serangan dengan tingkat akurasi tinggi, meskipun masih terdapat sedikit mis-klasifikasi pada beberapa kelas serangan minor.

2. Convolutional Neural Network (CNN)

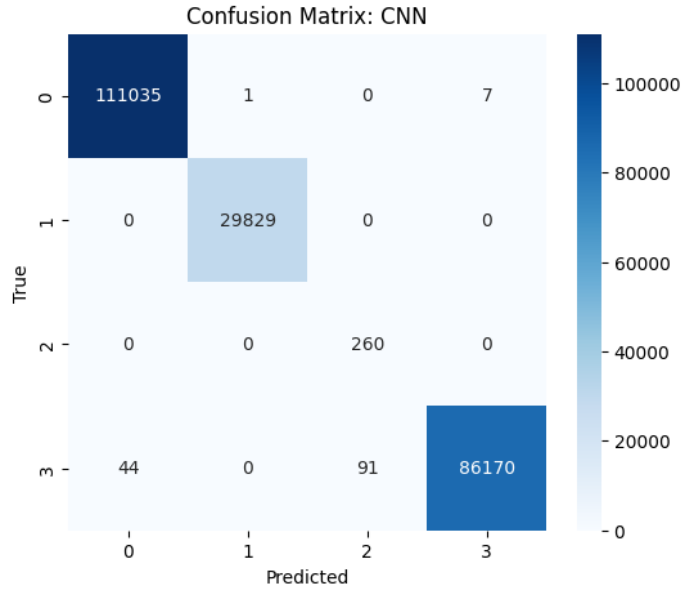
Convolutional Neural Network adalah algoritma *deep learning* yang efektif dalam mengenali pola kompleks. Dengan meniru mekanisme visual cortex manusia, CNN dapat mengekstraksi fitur penting dari data, sehingga mampu mendeteksi serangan dengan akurasi tinggi dan konsistensi yang lebih baik [13].CNN digunakan untuk mengekstraksi pola spasial dari *flow features* melalui operasi konvolusi 1D, sehingga mampu mengidentifikasi pola kompleks yang tidak tertangkap lapisan dense biasa.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727



Gambar 4. Plot Kurva Pelatihan Model CNN

Hasil pelatihan menunjukkan konvergensi yang cepat dengan penurunan loss yang signifikan pada epoch awal. Akurasi validasi stabil dan mendekati akurasi *training*.

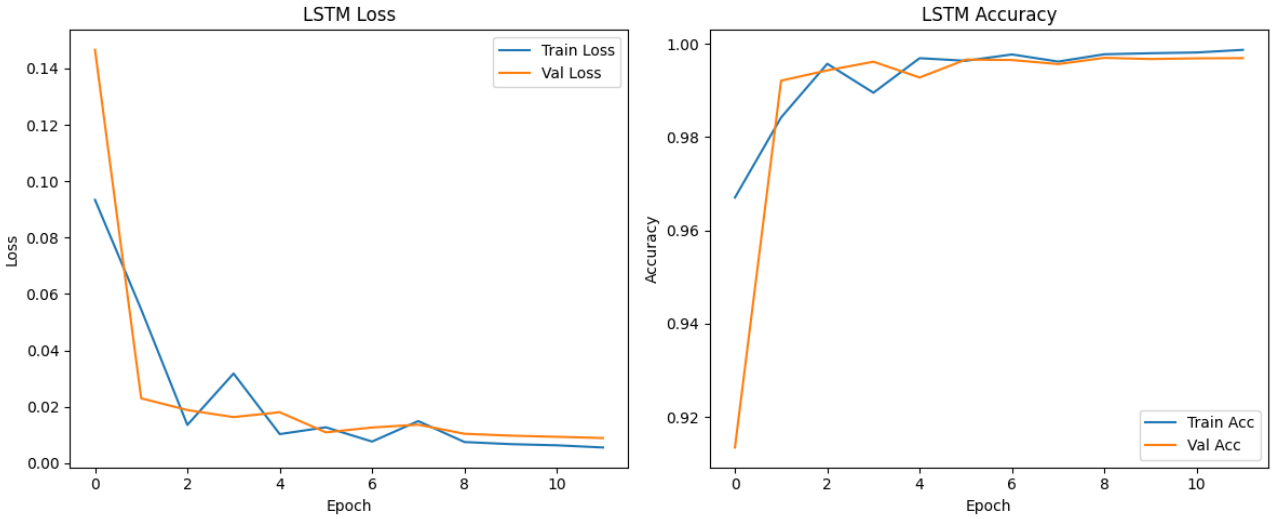


Gambar 5. *Confusion matrix* Model CNN

CNN menghasilkan tingkat klasifikasi yang sangat akurat dengan jumlah kesalahan lebih rendah dibandingkan DNN, terutama pada kelas serangan DDoS dengan pola trafik yang seragam.

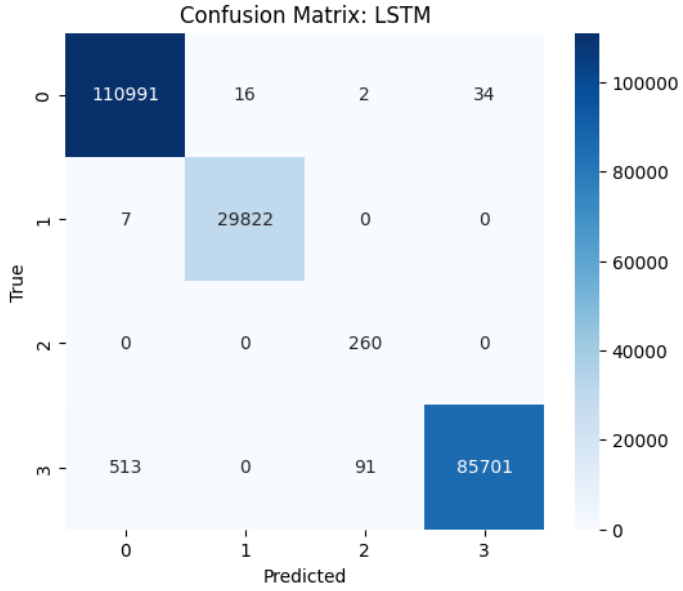
3. Long Short-Term Memory (LSTM)
   Long Short-Term Memory merupakan metode yang lebih unggul dibandingkan pendekatan konvensional, dan sangat sesuai untuk diterapkan dalam analisis sentimen [14]. LSTM digunakan untuk mempelajari ketergantungan jangka panjang pada urutan *flow features* yang direpresentasikan dalam bentuk sekuens.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727



Gambar 6. Plot Kurva Pelatihan Model LSTM

Kurva pelatihan menunjukkan pola belajar yang lebih fluktuatif dibandingkan DNN dan CNN, dengan proses konvergensi yang lebih lambat karena kompleksitas arsitektur sekuensial.



Gambar 7. Confusion matrix Model LSTM

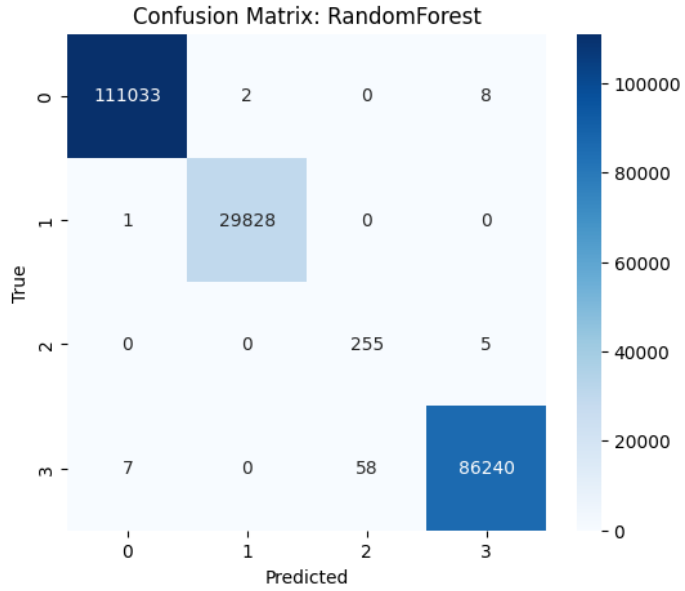
LSTM tetap mencapai performa tinggi dengan kesalahan klasifikasi yang relatif rendah, meskipun sedikit lebih besar dibandingkan CNN dan DNN karena sifat data flow yang kurang berurutan.

b. Model Machine learning sebagai Pembanding

1. Random Forest (RF)

Random Forest adalah metode *ensemble learning* yang menggabungkan beberapa *decision tree* untuk melakukan klasifikasi. Setiap pohon dibangun secara independen dengan pemilihan atribut acak pada node, dan prediksi akhir ditentukan melalui agregasi hasil dari semua pohon, sehingga meningkatkan akurasi dan kestabilan model. [15]. Random Forest digunakan sebagai baseline berbasis ensemble yang umum digunakan dalam deteksi intrusi jaringan karena kemampuannya menangani fitur tabular dan non-linear.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727

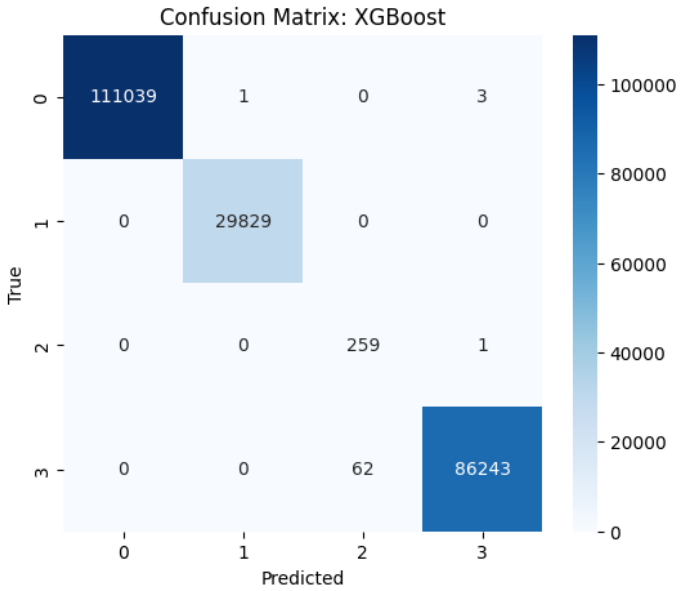


Gambar 8. Confusion matrix Model Random Forest

Confusion matrix menunjukkan bahwa RF mampu mengklasifikasikan sebagian besar trafik dengan akurasi tinggi. Meskipun demikian, performanya sedikit lebih rendah dibanding model *deep learning*, terutama pada kelas minor.

2. XGBoost

XGBoost adalah algoritma yang dikembangkan dari *gradient boosting decision tree* (GBDT), mampu membangun pohon keputusan secara *boosted* dengan efisiensi tinggi dan paralel, serta digunakan untuk menyelesaikan masalah klasifikasi dan regresi [16]. XGBoost digunakan sebagai baseline lanjutan berbasis boosting yang dirancang untuk performa tinggi pada data numerik berskala besar.



Gambar 9. Confusion matrix Model XGBoost

XGBoost mencapai performa sangat tinggi dan pada beberapa kelas mendekati kemampuan model *deep learning*, meskipun tetap terdapat sedikit mis-klasifikasi pada jenis serangan tertentu.

3.8 Evaluation

Tahap evaluasi dilakukan untuk menilai performa setiap model dalam mendeteksi serangan DDoS menggunakan *test set* sebesar 15% dari total data. Evaluasi dilakukan dengan menggunakan metrik utama berupa accuracy, precision, recall, dan F1-score. Hasil evaluasi seluruh model disajikan pada Tabel 5.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727

Tabel 5. Hasil Evaluasi

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DNN	99.9354	99.9476	99.9354	99.9389
CNN	99.9371	99.9475	99.9371	99.9401
LSTM	99.7085	99.7201	99.7085	99.7114
Random Forest	99.9644	99.9687	99.9644	99.9657
XGBoost	99.9705	99.9757	99.9705	99.9720

Berdasarkan Berdasarkan hasil evaluasi, seluruh model *deep learning* dan *machine learning* menunjukkan performa sangat tinggi dengan akurasi di atas 99%. *XGBoost* mencapai akurasi tertinggi sebesar 99,97%, diikuti *Random Forest* sebesar 99,96%. Pada kelompok *deep learning*, CNN memperoleh performa terbaik dengan akurasi 99,94%, disusul DNN, sementara LSTM mencatat akurasi terendah sebesar 99,71% meskipun tetap tergolong sangat baik. Secara keseluruhan, hasil ini menunjukkan bahwa kedua pendekatan mampu mendeteksi serangan *Distributed Denial of Service* (DDoS) secara efektif pada dataset CSE-CIC-IDS2018, dengan model berbasis *boosting* seperti XGBoost menunjukkan keunggulan akurasi, sehingga pemilihan model perlu disesuaikan dengan karakteristik data dan variasi serangan..

4. KESIMPULAN

Penelitian ini mengevaluasi kinerja tiga arsitektur *deep learning*, yaitu *Deep Neural Network (DNN)*, *Convolutional Neural Network (CNN)*, dan *Long Short-Term Memory (LSTM)*, dalam mendeteksi serangan *Distributed Denial of Service (DDoS)* berbasis *flow features* menggunakan dataset *CSE-CIC-IDS2018*. Selain itu, *Random Forest* dan *XGBoost* digunakan sebagai *baseline* pembanding untuk memberikan analisis performa yang lebih komprehensif antara pendekatan *deep learning* dan *machine learning* konvensional. Hasil eksperimen menunjukkan bahwa seluruh model mencapai tingkat akurasi di atas 99%, yang mengindikasikan bahwa representasi *flow-level features* efektif dalam membedakan trafik normal dan trafik serangan. Di antara model *deep learning*, *CNN* menunjukkan performa terbaik dengan akurasi sebesar 99,94% karena kemampuannya mengekstraksi pola spasial dari data tabular, diikuti oleh *DNN*, sementara *LSTM* memperoleh akurasi terendah sebesar 99,71% yang diduga disebabkan oleh keterbatasan data *flow-based* dalam merepresentasikan dependensi temporal jangka panjang. Di sisi lain, model *machine learning* berbasis *ensemble* menunjukkan performa yang sangat kompetitif, dengan *XGBoost* mencapai akurasi tertinggi sebesar 99,97% dan *Random Forest* sebesar 99,96%. Temuan ini menunjukkan bahwa keunggulan *deep learning* tidak selalu bersifat absolut, terutama pada data terstruktur yang relatif stabil. Namun demikian, penggunaan dataset terkontrol dengan tingkat *noise* rendah berpotensi menghasilkan evaluasi yang optimistis, sehingga penelitian lanjutan perlu menguji model pada skenario *real-time detection*, data dengan *noise* lebih tinggi, dan lingkungan jaringan nyata untuk menilai *robustness* dan kemampuan generalisasi sistem *Network Intrusion Detection System (NIDS)* secara lebih realistis.

REFERENCES

[1] S. Gamage and J. Samarabandu, "*Deep learning* methods in network intrusion detection: A survey and an objective comparison," *Journal of Network and Computer Applications*, vol. 169, p. 102767, Nov. 2020, doi: 10.1016/j.jnca.2020.102767.

[2] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A Survey of CNN-Based Network Intrusion Detection," *Applied Sciences*, vol. 12, no. 16, p. 8162, Aug. 2022, doi: 10.3390/app12168162.

[3] V. G. da Silva Ruffo *et al.*, "Anomaly and intrusion detection using *deep learning* for software-defined networks: A survey," *Expert Syst Appl*, vol. 256, p. 124982, Dec. 2024, doi: 10.1016/j.eswa.2024.124982.

[4] R. A. Widodo, M. K. Delimayanti, and A. Wulandari, "DDoS Attacks Detection With *Deep learning* Approach Using Convolutional Neural Network," *Journal of Applied Informatics and Computing*, vol. 8, no. 2, pp. 235–240, Aug. 2024, doi: 10.30871/jaic.v8i2.8242.

[5] V. P R and G. Paul, "A Survey on DDoS Attack Detection Methods Employing Intelligent Techniques," *International Journal of Computer Trends and Technology*, vol. 68, no. 11, pp. 83–85, Nov. 2020, doi: 10.14445/22312803/IJCTT-V68I11P113.

[6] M. Ouhssini, K. Afdel, M. Akouhar, E. Agherrabi, and A. Abarda, "Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches," *Egyptian Informatics Journal*, vol. 27, p. 100517, Sep. 2024, doi: 10.1016/j.eij.2024.100517.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 1639-1649
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.727

[7] S. Batool, M. Aslam, E. Akpokodje, and S. F. Jilani, "A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments: *Machine learning*, *Deep learning*, and Federated Learning Perspectives," *Electronics (Basel)*, vol. 14, no. 21, p. 4222, Oct. 2025, doi: 10.3390/electronics14214222.

[8] R. A. Widodo, M. K. Delimayanti, and A. Wulandari, "DDoS Attacks Detection With *Deep learning* Approach Using Convolutional Neural Network," *Journal of Applied Informatics and Computing*, vol. 8, no. 2, pp. 235–240, Aug. 2024, doi: 10.30871/jaic.v8i2.8242.

[9] M. Visca, R. Powell, Y. Gao, and S. Fallah, "Deep Meta-Learning Energy-Aware Path Planner for Unmanned Ground Vehicles in Unknown Terrains," *IEEE Access*, vol. 10, pp. 30055–30068, 2022, doi: 10.1109/ACCESS.2022.3155161.

[10] Y.-K. Kim and Y. Kim, "DiPLIP: Distributed Parallel Processing Platform for Stream Image Processing Based on *Deep learning* Model Inference," *Electronics (Basel)*, vol. 9, no. 10, p. 1664, Oct. 2020, doi: 10.3390/electronics9101664.

[11] J. L. Leevy and T. M. Khoshgoftaar, "A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data," *J Big Data*, vol. 7, no. 1, p. 104, Dec. 2020, doi: 10.1186/s40537-020-00382-x.

[12] M. Rizky, A. Pramuntadi, W. D. Prastowo, and D. H. Gutama, "Implementasi Metode Deep Neural Network pada Klasifikasi Penyakit Diabetes Melitus Tipe 2," *MALCOM: Indonesian Journal of Machine learning and Computer Science*, vol. 4, no. 3, pp. 1043–1050, Jun. 2024, doi: 10.57152/malcom.v4i3.1279.

[13] Kartiko, A. Prima Yudha, N. Dimas Aryanto, and M. Arya Farabi, "Klasifikasi Sampah di Saluran Air Menggunakan Algortima CNN," *Indonesian Journal of Data and Science*, vol. 3, no. 2, pp. 72–81, Jul. 2022, doi: 10.56705/ijodas.v3i2.33.

[14] Dedi Tri Hermanto, Arief Setyanto, and Emha Taufiq Luthfi, "Algoritma LSTM-CNN untuk Sentimen Klasifikasi dengan Word2vec pada Media Online," *Citec Journal*, vol. 8, no. 1, pp. 64–77, 2021.

[15] Suci Amaliah, M. Nusrang, and A. Aswi, "Penerapan Metode Random Forest Untuk Klasifikasi Varian Minuman Kopi di Kedai Kopi Konijiwa Bantaeng," *VARIANSI: Journal of Statistics and Its application on Teaching and Research*, vol. 4, no. 3, pp. 121–127, Dec. 2022, doi: 10.35580/variansiunm31.

[16] Ichwanul Muslim Karo Karo, "Implementasi Metode XGBoost dan Feature Importance untuk Klasifikasi pada Kebakaran Hutan dan Lahan," *Journal of Software Engineering, Information and Communication Technology*, vol. 1, no. 1, pp. 11–18, Nov. 2020.