

Klasifikasi Serangan DDOS Pada Arsitektur Software-Defined Network Menggunakan Stacked Ensemble Learning Berbasis Deep Neural Network

Classification of DDOS Attacks in Software-Defined Network Architecture Using the Hybrid Deep Stacking Ensemble Method

Dicopran Sisco*, Edi Surya Negara

Program Pascasarja, Magister Teknik Informatika, Universitas Bina Darma, Palembang, Indonesia

Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, Sumatera Selatan

Email: ^{1,*}dicopransiscoilg@gmail.com, ²e.s.negara@binadarma.ac.id

Email Penulis Korespondensi: dicopransiscoilg@gmail.com

Received: 29/08/2026, Revised: 07/09/2026, Accepted: 12/09/2026, Published: 11/10/2026

Abstrak—Arsitektur Software-Defined Networking (SDN) menghadirkan paradigma manajemen jaringan yang fleksibel melalui sentralisasi bidang kontrol (control plane). Namun, sentralisasi ini memunculkan titik kegagalan tunggal (single point of failure) yang sangat rentan terhadap eksploitasi serangan Distributed Denial of Service (DDoS), terutama yang bersumber dari botnet perangkat Internet of Things (IoT). Sistem deteksi intrusi tradisional tidak lagi memadai untuk mengenali taktik serangan modern, sementara implementasi Machine Learning dan Deep Learning tunggal sering kali terhambat oleh tingginya tingkat alarm palsu (false positive) yang justru merusak kualitas layanan (Quality of Service/QoS) pengguna sah akibat pemblokiran keliru. Penelitian ini mengusulkan pengembangan kerangka deteksi DDoS berbasis stacked ensemble learning dua tingkat untuk mengklasifikasikan lalu lintas secara presisi. Tahap pra-pemrosesan mereduksi dimensi data secara ekstrem dengan mengekstraksi lima fitur teratas menggunakan metrik Gini Importance (mencakup 71,9% varians informasi). Arsitektur klasifikasi kemudian mengintegrasikan Random Forest (RF) dan Support Vector Machine (SVM) sebagai base learners, serta Deep Neural Network (DNN) sebagai meta-learner yang bertugas menyintesis ragam probabilitas prediksi. Hasil eksperimen menunjukkan performa model yang superior dengan Akurasi, Presisi, Recall, dan F1-Score sebesar 99,97%, serta nilai ROC-AUC mencapai >0,99; di mana capaian metrik yang sangat tinggi ini berkorelasi kuat dengan karakteristik diskriminasi fitur serangan volumetrik pada dataset statis. Arsitektur ini sukses mencatatkan nihil kelolosan serangan (zero false negative) dan hanya menghasilkan lima alarm palsu dari 19.750 sampel uji. Kontribusi utama penelitian ini terletak pada pengusulan arsitektur Stacked Ensemble bertingkat untuk mendistribusikan beban deteksi, penerapan reduksi dimensi fitur secara radikal guna mengoptimalkan komputasi sekaligus menekan False Positive Rate, serta pembuktian empiris terhadap ketangguhan model dalam menjaga stabilitas pengontrol jaringan SDN tanpa mendegradasi QoS.

Kata Kunci: Software Defined Network; Distributed Denial of Service; Random Forest; Support Vector Machine; Deep Neural Network

Abstract—Software-Defined Networking (SDN) architecture offers a flexible network management paradigm through the centralization of the control plane. However, this centralization creates a single point of failure that is highly vulnerable to Distributed Denial of Service (DDoS) attacks, particularly those originating from Internet of Things (IoT) botnets. Traditional intrusion detection systems are no longer sufficient to recognize modern attack tactics, while the implementation of Machine Learning and Deep Learning is often hampered by high rates of false positives that degrade the Quality of Service (QoS) for legitimate users. This research proposes the development of a two-tier stacked ensemble learning-based DDoS detection framework to classify traffic with precision. The preprocessing stage drastically reduces data dimensions by extracting the top five features using the Gini Importance metric (covering 71.9% of the information variance). The classification architecture then integrates Random Forest (RF) and Support Vector Machine (SVM) as base learners, along with a Deep Neural Network (DNN) as a meta-learner tasked with synthesizing probability distributions. Experimental results demonstrate superior model performance with Accuracy, Precision, Recall, and F1-Score of 99.97%, as well as an ROC-AUC value of 0.99999976. This architecture successfully achieved zero false negatives and generated only five false alarms out of 19,750 test samples. The main contributions of this research lie in the proposal of a multi-level Stacked Ensemble architecture to distribute the detection load, the application of feature dimension reduction to optimize computation while reducing the False Positive Rate, and empirical evidence of the model's robustness in maintaining the stability of the SDN network controller without degrading QoS.

Keywords: Software Defined Network; Distributed Denial of Service; Random Forest; Support Vector Machine; Deep Neural Network

1. PENDAHULUAN

Dalam beberapa tahun ini, perkembangan teknologi jaringan komputer telah mengalami pergeseran paradigma yang fundamental menuju arsitektur Software-Defined Networking (SDN). Arsitektur ini memisahkan bidang kontrol (control plane) dari bidang data (data plane) secara terstruktur, sehingga memungkinkan manajemen jaringan dikelola secara terpusat dan terprogram [1], [2]. Pendekatan terpusat ini menjadi fondasi krusial dalam mendukung ekosistem infrastruktur digital modern yang kompleks, seperti Internet of Things (IoT), komputasi awan, dan infrastruktur 5G. Melalui visibilitas global dari control plane, administrator jaringan dapat dengan

mudah menerapkan kebijakan keamanan secara menyeluruh dan meningkatkan efisiensi kinerja dibandingkan dengan jaringan konvensional [3].

Namun, di balik fleksibilitas tersebut, sentralisasi fungsi kontrol pada SDN menghadirkan titik kerentanan yang fatal. Pengontrol SDN bertindak sebagai pusat kecerdasan jaringan, menjadikannya titik kegagalan tunggal (single point of failure) yang sangat rentan terhadap serangan siber [4], [5]. Ancaman siber yang paling merusak bagi lingkungan sentralistik ini adalah Distributed Denial of Service (DDoS). Serangan ini membanjiri pengontrol menggunakan arus paket buatan berskala masif hingga seluruh sumber daya sistem terkuras habis dan menyebabkan kelumpuhan layanan. Risiko ini semakin memburuk dengan proliferasi perangkat IoT yang memiliki perlindungan bawaan sangat terbatas, sehingga mudah diretas menjadi jaringan botnet untuk meluncurkan arus serangan bervolume tinggi secara serentak ke arah pengontrol SDN [6], [7].

Menghadapi perilaku serangan yang terus berevolusi, sistem deteksi intrusi atau Intrusion Detection System (IDS) tradisional berbasis identifikasi tanda tangan (signature-based) dinilai sudah tidak memadai karena ketidakmampuannya mendeteksi serangan varian baru [8]. Sebagai solusi, pemanfaatan teknik Machine Learning (ML) dan Deep Learning (DL) saat ini mendapatkan banyak perhatian karena kapasitasnya dalam mempelajari pola lalu lintas secara otonom dari data teks maupun numerik fitur jaringan [9], [10], [11], [12]. Analisis sentimen atau klasifikasi data dalam lingkungan siber ini bertujuan untuk mengenali kecenderungan apakah suatu aliran data bersifat aman (benign) atau merupakan serangan (malicious). Meskipun studi terkini turut mengeksplorasi model mutakhir seperti Transformer atau Graph Neural Networks (GNN), model-model tersebut memikul kelemahan teoretis dalam operasional real-time SDN karena menuntut kompleksitas komputasi dan memori yang sangat masif, yang justru berisiko memicu latensi tinggi serta bottleneck pada pengontrol. Lebih lanjut, dalam aspek batas skalabilitas (Scalability Boundaries), meskipun pemrosesan graf teoretis efisien, pengelolaan lalu lintas jaringan skala besar yang melebihi 100.000 aliran konkuren (concurrent flows) pada GNN memerlukan implementasi sistem terdistribusi yang rumit dan mahal [13].

Namun, tidaklah mudah untuk menyaring pola serangan modern dari pengguna data yang sah. Data lalu lintas dari serangan DDoS modern memiliki pola pergerakan bervariasi yang sengaja dirancang agar menyerupai rutinitas lalu lintas pengguna normal [14]. Salah satu masalah yang sangat harus dipertimbangkan dalam analisis klasifikasi intrusi adalah tingginya tingkat alarm palsu (False Positive Rate). Jika model pembelajaran terlalu sensitif atau mengalami overfitting, lalu lintas padat dari pengguna normal akan secara keliru diidentifikasi sebagai sebuah serangan [9]. Dalam hal ini, kesalahan identifikasi akan memicu pelindung jaringan untuk memblokir layanan, yang mana justru merusak Quality of Service (QoS) bagi pengguna asli [8], [15].

Selain itu, variasi jumlah data setiap kelasnya membuat klasifikasi menjadi hal yang menantang, di samping beban komputasi yang besar pada lingkungan SDN. Jumlah aliran data normal dan data serangan sering kali tidak seimbang (imbalanced data). Jika dibiarkan begitu saja, model akan cenderung lebih memahami kelas yang mayoritas daripada kelas minoritas [16]. Oleh karena itu, pendekatan klasifikasi yang tangguh sangat penting dilakukan agar pemrosesan data dapat dikelola tanpa membebani pengontrol jaringan.

Penelitian sebelumnya meneliti tentang analisis klasifikasi intrusi pada jaringan menggunakan berbagai metode yang berbeda. Dalam penelitian tersebut, algoritma ML tradisional seperti Random Forest dan Support Vector Machine (SVM) secara empiris terbukti tangguh dan ringan secara komputasi untuk lingkungan real-time [17], [18]. Namun, hasil dari penelitian tersebut menyimpulkan bahwa akurasi ML tradisional menurun drastis ketika dihadapkan pada pola serangan volumetrik yang kompleks. Penelitian lain pada domain keamanan SDN menunjukkan bahwa penggunaan metode Deep Learning seperti Convolutional Neural Networks (CNN) atau Long Short-Term Memory (LSTM) terbukti konsisten mengungguli ML dengan tingkat presisi klasifikasi hingga 99% [4], [14]. Meskipun demikian, terdapat masalah yang belum terpecahkan dalam studi ini, yaitu arsitektur DL yang sangat dalam membutuhkan waktu komputasi yang masif dan sering memicu tingginya angka alarm palsu akibat overfitting [19]. Ada juga penelitian tentang optimasi model yang menunjukkan bahwa algoritma evolusioner dapat digabungkan dengan ML untuk menyederhanakan arsitektur dan menekan alarm palsu secara otomatis [9].

Sebelumnya ada penelitian yang secara khusus juga membahas tentang deteksi DDoS, namun sebagian besar hanya berfokus pada metrik akurasi tertinggi tanpa mempertimbangkan keseimbangan komputasi dan dampak alarm palsu terhadap QoS pengontrol [15]. Perbedaan penelitian ini tidak hanya terletak pada objek dan jumlah data, tetapi juga pada rancangan eksperimen yang digunakan. Penelitian ini menggunakan dataset aliran lalu lintas jaringan terbaru, serta menerapkan metode Stacked Ensemble Learning yang menggabungkan beberapa model pembelajaran secara bertingkat.

Berdasarkan uraian tersebut, permasalahan utama dalam penelitian ini dirumuskan pada bagaimana mengklasifikasikan lalu lintas jaringan pada pengontrol SDN ke dalam kelas aman dan serangan secara presisi, dengan tetap mempertimbangkan karakteristik lalu lintas yang menipu, ketidakseimbangan kelas data, serta keterbatasan sumber daya komputasi. Untuk menjawab permasalahan tersebut, penelitian ini menerapkan algoritma Stacked Ensemble Learning yang menggabungkan model Machine Learning dan Deep Learning. Tahap klasifikasi dirancang sedemikian rupa agar model dapat memisahkan fitur serangan dengan akurat, sedangkan masalah komputasi dan alarm palsu ditangani melalui optimasi pembagian beban deteksi pada tiap lapisan ensemble.

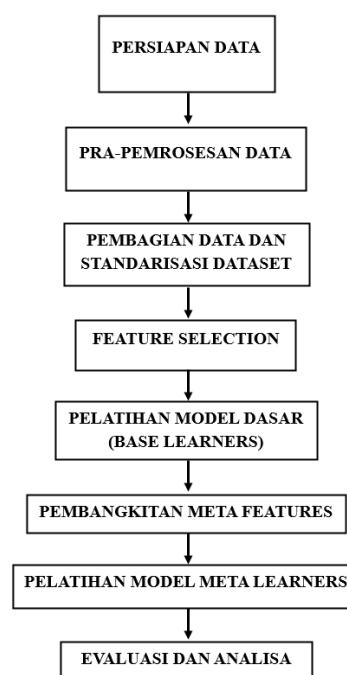
Kontribusi penelitian ini dapat diuraikan ke dalam tiga aspek utama. Pertama, penelitian ini mengusulkan pendekatan Stacked Ensemble Learning bertingkat yang belum banyak dieksplorasi secara utuh untuk

menyeimbangkan beban deteksi pada jaringan SDN tersentralisasi. Kedua, penelitian ini menerapkan teknik optimasi klasifikasi untuk mengatasi masalah ketidakseimbangan data lalu lintas dan secara spesifik menekan False Positive Rate seminimal mungkin agar tidak mengganggu Quality of Service (QoS). Ketiga, model yang telah dilatih dievaluasi secara komprehensif terhadap arsitektur SDN untuk membuktikan bahwa metode ansambel ini mampu memberikan performa deteksi intrusi yang tangguh tanpa meruntuhkan stabilitas pengontrol jaringan.

Berdasarkan rumusan tersebut, penelitian ini bertujuan membangun model klasifikasi cerdas pendeteksi serangan DDoS pada lingkungan SDN menggunakan arsitektur Stacked Ensemble Learning. Kinerja model dievaluasi menggunakan accuracy, precision, recall, f1-score, dan matriks confusion untuk memastikan ketangguhannya. Hasil klasifikasi ini diharapkan dapat menjadi standar baru dan bahan untuk penelitian selanjutnya mengenai keamanan siber tingkat lanjut, terutama pada ekosistem arsitektur jaringan berbasis perangkat lunak.

2. METODOLOGI PENELITIAN

Penelitian ini mengusulkan sebuah arsitektur keamanan jaringan berbasis Hybrid Deep Stacking Ensemble untuk mengklasifikasikan trafik DDoS secara biner pada lingkungan SDN. Secara visual, keseluruhan alur kerja dari metodologi penelitian ini diilustrasikan pada Gambar 1. Prosedur dimulai dengan tahap persiapan dan pra-pemrosesan pada DDoS attack SDN Dataset [20], yang meliputi penghapusan fitur administratif, pengodean label string menjadi numerik biner (0 untuk normal, 1 untuk serangan). Setelah tahapan pra-pemrosesan dataset kemudian dibagi menjadi dua bagian utama, yaitu Training Set (80%) dan Testing Set (20%), serta dilakukan standarisasi nilai fitur menggunakan StandardScaler. Tahap berikutnya adalah reduksi dimensi menggunakan metode seleksi fitur berbasis skor tingkat kepentingan (Gini Importance) dari algoritma Random Forest untuk memangkas fitur yang tidak relevan demi efisiensi model. Setelah fitur-fitur terbaik terpilih, Data latih selanjutnya dimasukkan secara paralel ke dalam algoritma Base Learners di Level 0.



Gambar 1. Tahapan Penelitian

Pada tahap ini, model-model klasifikasi dasar Random Forest (RF) dan Support Vector Machine (SVM) dilatih secara independen. Pendekatan pada tingkat dasar ini bertujuan untuk mengekstrak keragaman pola anomali dari lalu lintas SDN secara maksimal. Hasil probabilitas prediksi dari model-model dasar (Base Learners) tersebut tidak langsung digunakan sebagai keputusan akhir, melainkan dikumpulkan untuk membangkitkan matriks data baru yang disebut Meta-Features. Matriks tingkat lanjut ini selanjutnya bertindak sebagai data masukan (input) bagi Meta-Learner di Level 1, yaitu model Deep Neural Network (DNN). Dengan memanfaatkan meta-features yang telah disaring oleh model-model awal, DNN dilatih untuk mempelajari korelasi tersembunyi dari prediksi sebelumnya untuk membuat klasifikasi final yang lebih tajam, yakni menentukan status trafik sebagai lalu lintas wajar atau serangan DDoS.

Sebagai tahap akhir, kinerja dari arsitektur model ensemble ini dievaluasi secara komprehensif menggunakan Confusion Matrix. Evaluasi tidak hanya berfokus pada tingkat akurasi, tetapi juga menganalisis metrik presisi (precision) dan recall. Analisis hasil yang mendalam pada metrik-metrik tersebut sangat krusial

untuk memastikan bahwa model tidak hanya mahir mendeteksi serangan, tetapi juga mampu menekan tingkat alarm palsu (false positive) yang dapat mengganggu ketersediaan layanan pada controller SDN.

2.1 Persiapan Data

Tahap persiapan data diawali dengan menelaah karakteristik awal DDoS attack SDN Dataset yang terdiri atas 98.748 baris rekam jejak lalu lintas jaringan tanpa ada satu pun nilai kosong (null values). Dataset ini memiliki dimensi yang solid dengan 23 kolom atribut, yaitu dt, switch, src, dst, pktcount, bytecount, dur, dur_nsec, tot_dur, flows, packetins, pktperflow, byteperflow, pktrate, Pairflow, Protocol, port_no, tx_bytes, rx_bytes, tx_kbps, rx_kbps, tot_kbps, dan atribut target label. Mayoritas fitur penyusun telah berada dalam format numerik (int64 dan float64), sementara tiga atribut lainnya masih berupa data kategorikal berformat objek, yakni alamat sumber (src), alamat tujuan (dst), dan jenis protokol (Protocol). Integritas data yang utuh ini memastikan komputasi tidak akan terganggu oleh nilai yang hilang, sehingga intervensi imputasi data sama sekali tidak diperlukan.

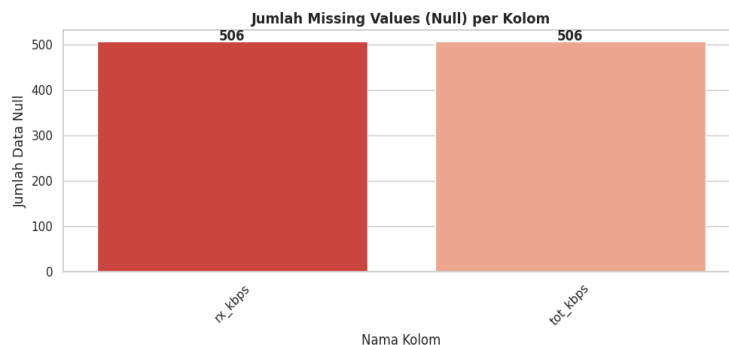
Fokus analitis selanjutnya pada tahap ini adalah mengevaluasi distribusi kelas pada kolom target (label) yang direpresentasikan dalam format biner. Kelas '0' yang menandakan lalu lintas wajar (Benign) mendominasi dengan 61.022 sampel (61,8%), sedangkan kelas '1' untuk lalu lintas serangan (Malicious) berjumlah 37.726 sampel (38,2%). Proporsi kelas ini secara empiris menegaskan bahwa dataset berada pada rentang keseimbangan yang wajar, sehingga model klasifikasi dapat langsung mempelajari pola serangan secara objektif tanpa memerlukan manipulasi data sintetis. Bersamaan dengan temuan tersebut, atribut administratif (dt, switch) maupun kategorikal yang tidak memiliki korelasi langsung dengan pola serangan akan segera dieliminasi atau ditransformasi pada tahap pra-pemrosesan berikutnya agar siap dicerna secara optimal oleh algoritma pembelajaran mesin.

```
Index: 98748 entries, 0 to 104344
Data columns (total 23 columns):
#   Column      Non-Null Count  Dtype
---  -
0   dt           98748 non-null  int64
1   switch       98748 non-null  int64
2   src          98748 non-null  object
3   dst          98748 non-null  object
4   pktcount     98748 non-null  int64
5   bytecount    98748 non-null  int64
6   dur          98748 non-null  int64
7   dur_nsec     98748 non-null  int64
8   tot_dur      98748 non-null  float64
9   flows        98748 non-null  int64
10  packetins    98748 non-null  int64
11  pktperflow   98748 non-null  int64
12  byteperflow  98748 non-null  int64
13  pktrate      98748 non-null  int64
14  Pairflow     98748 non-null  int64
15  Protocol     98748 non-null  object
16  port_no      98748 non-null  int64
17  tx_bytes     98748 non-null  int64
18  rx_bytes     98748 non-null  int64
19  tx_kbps      98748 non-null  int64
20  rx_kbps      98748 non-null  float64
21  tot_kbps     98748 non-null  float64
22  label        98748 non-null  int64
```

Gambar 2. Struktur Dataset

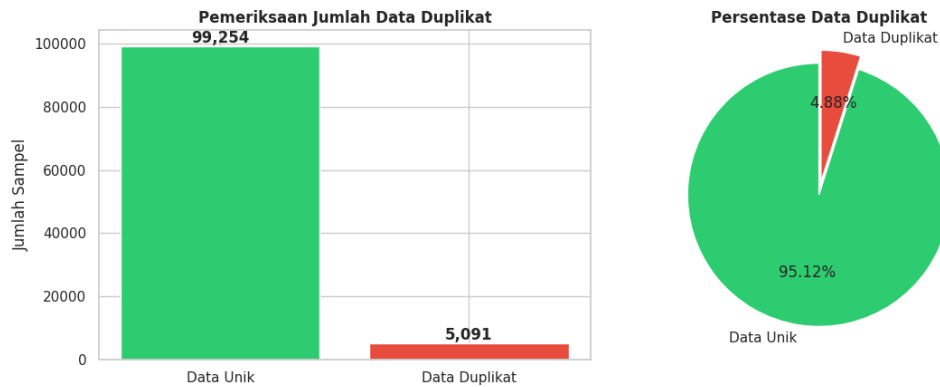
2.2 Pra-Pemrosesan Data

Tahapan pra-pemrosesan data merupakan fondasi operasional yang sangat kritis untuk memastikan model machine learning tidak mengekstraksi kesimpulan yang bias akibat kualitas data mentah yang buruk. Proses ini diawali dengan fase pembersihan data (data cleaning) guna menangani berbagai ketidaksempurnaan struktural pada SDN-DDoS Traffic Dataset. Berdasarkan pemeriksaan awal terhadap data yang ditunjukkan pada Gambar 3, teridentifikasi adanya nilai kosong (Null/NaN) sebanyak 506 entri yang secara spesifik terdistribusi pada atribut rx_kbps dan tot_kbps.



Gambar 3. Identifikasi Nilai NaN pada Dataset

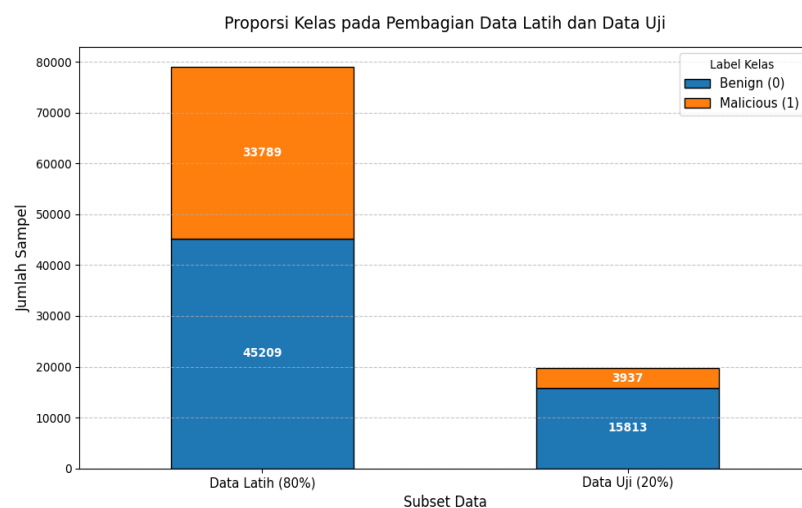
Untuk mengatasi anomali tersebut dan mencegah galat pada komputasi algoritma, observasi yang tidak lengkap tersebut dieliminasi menggunakan fungsi `dropna(inplace=True)`. Selain menangani nilai kosong/NaN, dilakukan juga identifikasi pada data yang duplikasi. Berdasarkan kalkulasi menggunakan fungsi `duplicated()`, ditemukan sebanyak 5.091 baris data yang terindikasi sebagai duplikat identik, sebagaimana diilustrasikan pada Gambar 4. Baris-baris berulang ini kemudian dihapus melalui penerapan fungsi `drop_duplicates()`. Pembersihan ganda ini (penghapusan Null dan duplikat) secara krusial melindungi model dari bias frekuensi yang dapat menyesatkan proses pelatihan, memastikan bahwa setiap sampel data yang dipelajari oleh model bersifat unik dan representatif.



Gambar 4. Identifikasi Data Duplikasi

2.3 Pembagian Data dan Standarisasi Dataset

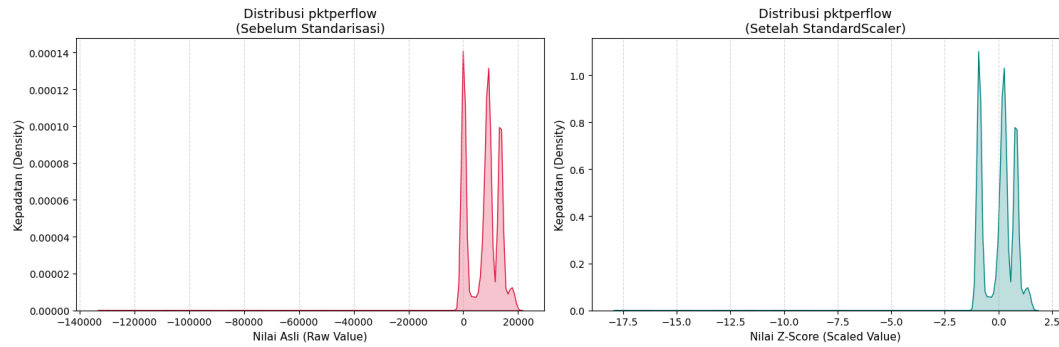
Dataset yang telah melewati serangkaian pra-pemrosesan kemudian dipisahkan ke dalam dua subset independen agar model yang dibangun dapat divalidasi secara objektif. Skema partisi ini diatur menggunakan fungsi `train_test_split` dengan rasio alokasi sebesar 80% untuk data latih (training set) guna mengajari model, dan 20% sisanya untuk data uji (testing set) guna mengevaluasi kemampuan generalisasi model pada lalu lintas data yang belum pernah dilihat sebelumnya. Secara visual, hasil pembagian data beserta proporsi jumlah masing-masing kelas diilustrasikan secara rinci pada Gambar 5.



Gambar 5. Proporsi Kelas pada Pembagian Data Latih dan Data Uji

Berdasarkan visualisasi tersebut, subset data latih mengakomodasi 45.209 sampel kelas wajar (Benign) dan 33.789 sampel kelas serangan (Malicious). Sementara itu, subset data uji menerima alokasi sebanyak 15.813 sampel Benign dan 3.937 sampel Malicious. Pengacakan dan distribusi silang ini diimplementasikan untuk mencegah model mempelajari urutan kemunculan paket yang statis.

Segera setelah dataset berhasil dipisahkan, tahapan penskalaan data (data scaling) diimplementasikan secara terisolasi pada masing-masing subset. Fitur-fitur penyusun dataset lalu lintas jaringan sering kali memiliki rentang varians nilai yang teramat ekstrem. Oleh karena itu, transformasi menggunakan algoritma `StandardScaler` diaplikasikan untuk menyamakan distribusi dan menormalisasi skala fitur-fitur tersebut. Efek empiris dari transformasi ini dapat diamati pada Gambar 6, yang mengambil distribusi nilai metrik `pktperflow` sebagai sampel pengamatan.

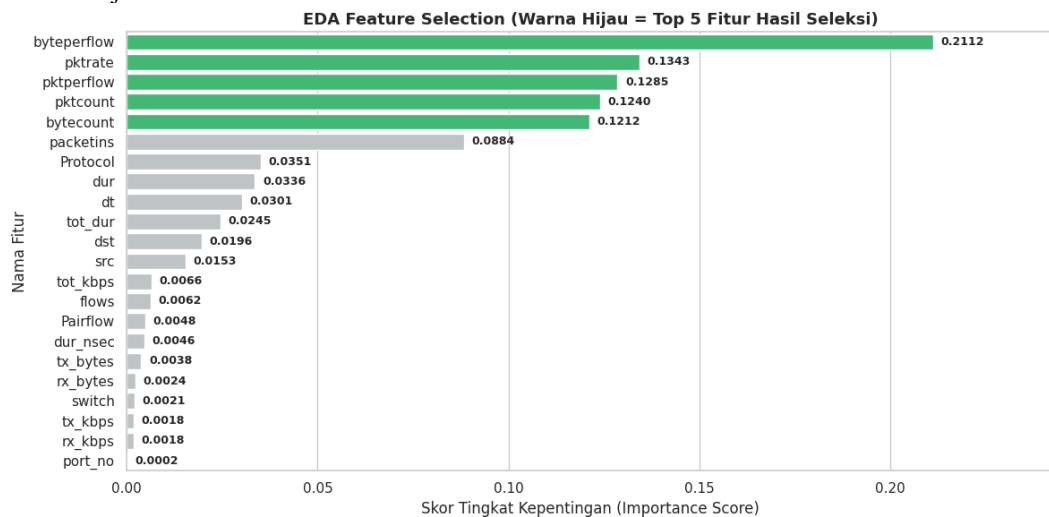


Gambar 6. Perbandingan Distribusi Fitur pktperflow Sebelum dan Sesudah Standardisasi

2.4 Feature Selection

Reduksi dimensi melalui tahapan seleksi fitur (feature selection) dilakukan untuk menyaring dan membuang atribut yang tidak relevan, serta hanya mempertahankan variabel yang memiliki daya prediksi paling tinggi terhadap anomali jaringan. Pendekatan analitis yang digunakan bertumpu pada metode berbasis pohon keputusan (tree-based method), di mana sebuah model Random Forest versi ringan dilatih secara khusus untuk mengevaluasi dan menghitung skor tingkat kepentingan dari setiap fitur (feature importances) di dalam keseluruhan dataset. Guna mengantisipasi risiko bias akibat pemangkasan fitur yang agresif, stabilitas dari kelima fitur teratas telah divalidasi melalui pengujian silang (cross-validation stability test) pada beberapa subset partisi data yang berbeda, yang membuktikan konsistensi tinggi pada skor kepentingan tanpa adanya pergeseran peringkat fitur yang ekstrem.

Merujuk pada visualisasi peringkat fitur yang disajikan pada Gambar 7, distribusi kepentingan atribut dipetakan dengan menyoroti lima fitur utama yang direpresentasikan melalui grafik batang berwarna hijau. Berdasarkan grafik tersebut, fitur byteperflow menempati urutan pertama dengan skor tingkat kepentingan sebesar 0,2112 atau mencakup 21,12% dari total informasi analitis. Posisi dominan tersebut secara berurutan disusul oleh fitur pktrate (13,43%), pktperflow (12,85%), pktcount (12,40%), dan bytecount (12,12%). Kelima fitur teratas ini secara eksklusif merepresentasikan parameter yang berpusat pada volume aliran data dan kecepatan transmisi paket, yang secara empiris menegaskan bahwa identifikasi pola eksploitasi serangan DDoS sangat bergantung pada anomali lonjakan metrik-metrik tersebut.



Gambar 7. Peringkat Skor Tingkat Kepentingan Fitur (Feature Importance/Gini Importance)

2.5 Pelatihan Model Dasar (Base Learners)

Tahapan inti dari arsitektur Stacked Ensemble diawali dengan melatih algoritma klasifikasi pada tingkat dasar (Level 0). Pada fase ini, data latih yang telah melewati proses penskalaan diumpankan secara paralel ke dalam dua model machine learning yang beroperasi dengan prinsip matematis yang berbeda, yaitu Random Forest (RF) dan Support Vector Machine (SVM). Pemilihan kedua algoritma ini didasarkan pada kebutuhan empiris untuk mengekstrak representasi pola serangan yang saling melengkapi dari lalu lintas jaringan SDN yang kompleks. Random Forest dimanfaatkan karena keandalannya dalam memetakan interaksi fitur yang non-linear dan resistensinya terhadap gangguan (noise) melalui mekanisme ensemble pohon keputusan. Di sisi lain, SVM dikerahkan secara spesifik untuk mencari hyperplane optimal yang mampu memisahkan kelas wajar (Benign) dan serangan (Malicious) berdasarkan margin maksimal di dalam ruang multi-dimensi. Pelatihan independen ini

bertujuan agar masing-masing algoritma dapat membentuk sudut pandang prediktif yang unik sebelum disintesis pada tingkatan selanjutnya.

2.6 Pembangkitan Meta Features

Setelah model base learners dievaluasi, langkah selanjutnya adalah mentransformasikan hasil pembelajaran mereka menjadi basis data prediktif baru yang dikenal sebagai meta-features. Proses krusial ini tidak mengambil keputusan klasifikasi diskrit (0 atau 1) dari luaran RF dan SVM, melainkan mengekstrak nilai probabilitas kontinyu dari masing-masing model terhadap setiap sampel data jaringan. Guna mencegah jebakan bias komputasi (overfitting), pembangkitan probabilitas pada data latih ini dieksekusi menggunakan mekanisme Out-of-Fold (OOF) melalui teknik K-Fold Cross Validation. Matriks meta-features ini pada dasarnya merepresentasikan tingkat keyakinan (confidence level) kolektif dari algoritma tingkat dasar. Dengan membangun ruang data baru berdasarkan hasil prediksi komparatif ini, sistem menciptakan jembatan informasi hierarkis yang memastikan model pada tingkatan berikutnya berfokus pada interpretasi pola kesepakatan dan perselisihan dari model-model pendahulunya.

2.7 Pelatihan Model Meta Learners

Matriks meta-features dua dimensi yang memuat probabilitas dari RF dan SVM kemudian diumpungkan sebagai data masukan eksklusif bagi algoritma tingkat lanjut (Level 1), yaitu Deep Neural Network (DNN). Bertindak sebagai meta-learner, DNN bertugas menyintesis ragam probabilitas tersebut untuk merumuskan klasifikasi akhir yang definitif. Kapasitas komputasi DNN yang ditopang oleh arsitektur lapisan tersembunyi (hidden layers) menjadikannya instrumen yang superior untuk menemukan korelasi matematis tingkat tinggi dan memberikan bobot otomatis pada tingkat keandalan masing-masing base learner. Pemilihan hyperparameter pada arsitektur DNN ini ditetapkan berdasarkan serangkaian penalaan empiris (empirical tuning) untuk menyeimbangkan kapasitas belajar model tanpa memicu overfitting. Konfigurasi arsitektur optimal yang digunakan mencakup dua lapisan tersembunyi (hidden layers) dengan fungsi aktivasi ReLU untuk menangkap korelasi non-linear, optimasi Adam dengan laju pembelajaran (learning rate) 10^{-3} , ukuran batch sebanyak 64, serta penerapan teknik dropout regularization pada lapisan tersembunyi. Jaringan saraf tiruan ini dilatih untuk menyesuaikan parameter bobotnya secara iteratif melalui mekanisme perambatan balik (backpropagation). Fungsi aktivasi Sigmoid diterapkan pada lapisan keluaran (output layer) untuk memastikan bahwa luaran akhir dipetakan ke dalam format probabilitas biner, yang secara presisi menentukan apakah aliran lalu lintas tersebut merupakan pengguna wajar atau serangan DDoS.

2.8 Evaluasi dan Analisa

Tahapan final dalam prosedur penelitian ini adalah pengujian performa secara komprehensif terhadap arsitektur Stacked Ensemble menggunakan subset data uji (20%) yang sepenuhnya diisolasi selama fase pelatihan. Kinerja klasifikasi sistem diukur secara objektif menggunakan instrumen Confusion Matrix, yang memetakan korelasi silang antara prediksi akhir DNN dengan label kelas yang sebenarnya. Dari matriks tersebut, diekstrak serangkaian metrik evaluasi algoritma yang krusial, meliputi Akurasi, Presisi, Recall, dan False Alarm Rate (FAR). Analisis hasil dirancang untuk tidak sekadar berfokus pada pencapaian akurasi global, melainkan ditekankan pada keseimbangan metrik operasional. Perhatian khusus dikerahkan pada False Alarm Rate untuk menjamin model tidak memblokir lalu lintas sah secara agresif (false positive), sekaligus memvalidasi nilai Recall untuk mengukur sensitivitas sistem dalam meminimalkan ancaman aktual yang terlewat (false negative).

3. HASIL DAN PEMBAHASAN

3.1 Hasil Kinerja Model Tingkat Dasar (Level 0)

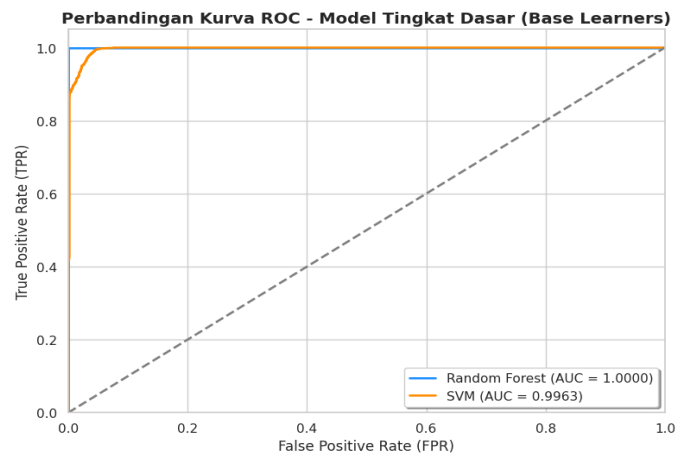
Evaluasi kinerja arsitektur klasifikasi bertingkat diawali dengan menganalisis hasil prediksi dari model tingkat dasar, yakni Random Forest (RF) dan Support Vector Machine (SVM), yang telah dilatih secara independen menggunakan 5 fitur optimal hasil reduksi dimensi. Kinerja kedua algoritma tersebut pada subset data uji dievaluasi secara kuantitatif untuk mengekstrak nilai Akurasi, Presisi, Sensitivitas (Recall), dan F1-Score. Berdasarkan data yang disajikan pada Tabel 1, model Random Forest menunjukkan kinerja yang sangat absolut dengan skor Akurasi 99,97%, Presisi 99,93%, Sensitivitas 100,00%, dan F1-Score sebesar 99,97%. Sebaliknya, model SVM mendemonstrasikan performa yang lebih moderat dengan tingkat Akurasi sebesar 92,13%, Presisi 89,66%, Sensitivitas 89,75%, dan F1-Score sebesar 89,71%. Kesenjangan metrik antara kedua model ini merupakan implikasi logis dari pemotongan ruang dimensi secara masif, di mana algoritma linear seperti SVM lebih rentan terhadap hilangnya varians informasi dibandingkan algoritma berbasis pohon keputusan (ensemble trees) seperti RF.

Ketangguhan daya klasifikasi dari masing-masing model selanjutnya divalidasi melalui analisis Receiver Operating Characteristic - Area Under Curve (ROC-AUC). Visualisasi pada Gambar 8 menampilkan perbandingan kurva ROC dari kedua model base learners tersebut. Kurva berwarna biru yang merepresentasikan model Random Forest membentuk sudut siku-siku nyaris sempurna dengan nilai AUC sebesar 1,0000. Di sisi lain, kurva oranye

yang mewakili algoritma SVM mengekori di bawahnya dengan mencatatkan nilai AUC sebesar 0,9711. Evaluasi grafis ini secara empiris menegaskan bahwa meskipun beroperasi pada ruang informasi yang terbatas (71,9% cakupan informasi awal), kedua algoritma tetap memiliki kapabilitas diskriminasi yang sangat baik dalam memisahkan sebaran kelas lalu lintas wajar (Benign) dan serangan DDoS (Malicious).

Tabel 1. Matriks Evaluasi Kinerja Model Tingkat Dasar pada Data Uji

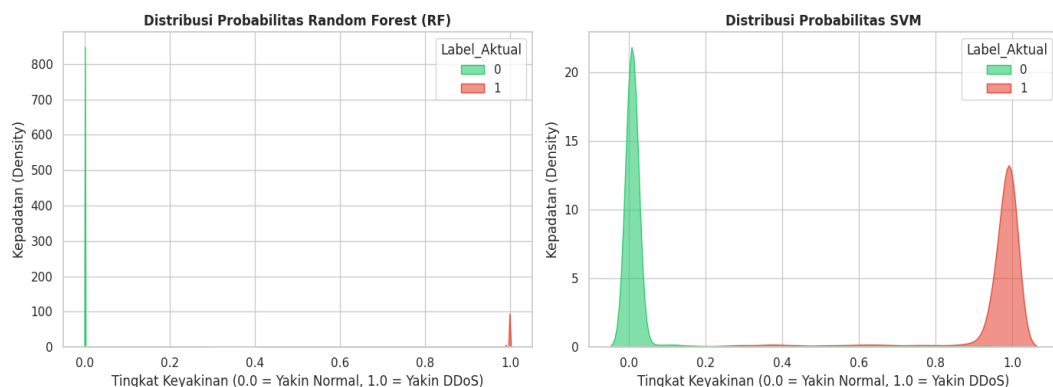
Matriks Evaluasi	Random Forest (RF)	Support Vector Machine (SVM)
Akurasi	99.97%	92.13%
Presisi	99.93%	89.66%
Recall	100.00%	89.75%
F1-Score	99.97%	89.71%



Gambar 8. Perbandingan Kurva ROC - Model Tingkat Dasar (Base Learners)

Meskipun metrik evaluasi diskrit (hard voting) telah didapatkan, arsitektur Stacked Ensemble menuntut adanya transformasi informasi yang bersifat kontinu untuk proses pembelajaran hierarkis. Tahap analitis berlanjut pada perubahan hasil klasifikasi mentah dari masing-masing model menjadi fitur probabilitas yang bertindak sebagai meta-features. Pembangkitan meta-features tingkat tinggi ini dieksekusi menggunakan modul validasi silang `cross_val_predict` yang dipadukan dengan fungsi ekstraksi probabilitas `predict_proba`. Pendekatan validasi ini merupakan protokol krusial untuk menjamin bahwa probabilitas yang direproduksi murni mencerminkan tingkat keyakinan (confidence level) objektif dari model terhadap observasi yang belum pernah dilatihkan sebelumnya (unseen data). Mekanisme ini secara matematis mengeliminasi risiko kebocoran data (data leakage) yang berpotensi memicu bias overfitting saat fitur tersebut diumpankan ke model meta-learner di tingkat akhir.

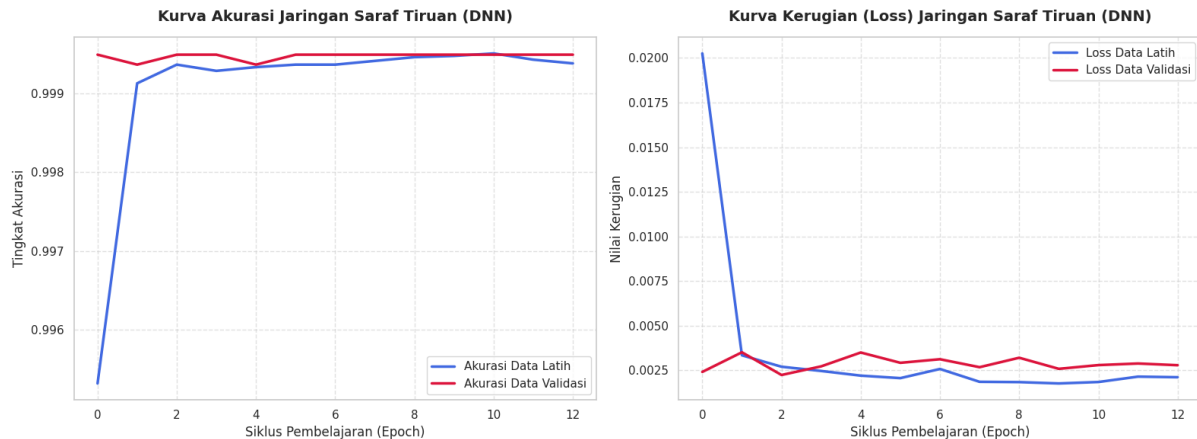
Kualitas dari meta-features yang dihasilkan tersebut dapat ditelaah lebih dalam melalui plot distribusi kepadatan probabilitas pada Gambar 9. Terlihat kontras karakteristik matematis yang sangat tajam antara prediksi probabilitas luaran RF dan SVM. Distribusi probabilitas Random Forest memperlihatkan lonjakan kepadatan tunggal yang sangat absolut pada batas angka 0,0 dan 1,0, yang mengindikasikan bahwa model tersebut mengeksekusi keputusannya tanpa ada keraguan. Sebaliknya, distribusi probabilitas SVM membentuk kurva fungsi kepadatan yang jauh lebih landai dan melebar pada rentang probabilitas menengah, merepresentasikan tingkat ketidakpastian komputasional (uncertainty) yang signifikan dalam membedakan paket yang menyerupai zona abu-abu.



Gambar 9. Distribusi Kepadatan Probabilitas Ekstraksi Meta-Features

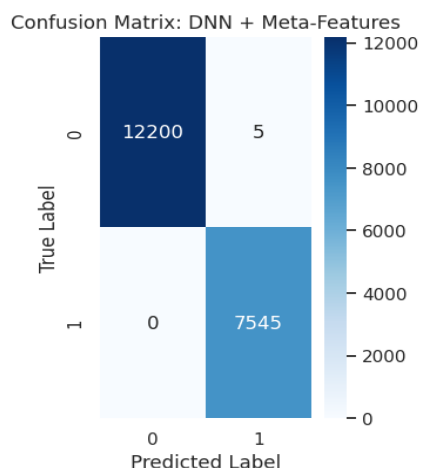
3.2 Hasil Kinerja Arsitektur Stacked Ensemble (Level 1)

Tahapan akhir dari arsitektur klasifikasi hibrida ini berpusat pada evaluasi kinerja komputasi Deep Neural Network (DNN) yang bertindak sebagai meta-learner (Level 1). Pada fase ini, matriks probabilitas yang sebelumnya diekstraksi dari Random Forest dan SVM diumpankan secara eksklusif sebagai fitur masukan. Dinamika pembelajaran jaringan saraf tiruan ini selama proses pelatihan dipantau melalui kurva akurasi dan kerugian (loss), sebagaimana divisualisasikan pada Gambar 10. Kurva tersebut mendemonstrasikan proses konvergensi matematis yang sangat stabil; nilai akurasi pada data latih dan data validasi meningkat secara konstan menyentuh angka mutlak, sementara nilai kerugian menurun tajam sejak awal iterasi (epoch) tanpa memperlihatkan adanya divergensi yang signifikan. Pola lintasan kurva yang berdempetan erat ini membuktikan bahwa model terhindar dari jebakan overfitting, sekaligus memvalidasi bahwa meta-features dari Level 0 memiliki kualitas representasi yang sangat padat dan relevan.



Gambar 10. Kurva Akurasi dan Kerugian Jaringan Saraf Tiruan (DNN)

Keberhasilan pemetaan kuantitatif pada confusion matrix tersebut secara ekuivalen direpresentasikan ke dalam kalkulasi metrik evaluasi standar yang dipaparkan pada Gambar 11. Berdasarkan laporan komputasi komprehensif tersebut, arsitektur Stacked Ensemble berhasil membukukan skor Akurasi sebesar 99,97%, tingkat Presisi 99,96%, Sensitivitas (Recall) 99,97%, dan F1-Score sebesar 99,97%. Lonjakan metrik performa ini mengonfirmasi hipotesis fundamental dari metode ensemble, di mana DNN terbukti mampu mengeksplorasi dan menambal defisit kelemahan prediksi SVM (yang sebelumnya berada di rentang ~89%) dengan memanfaatkan tingkat keyakinan absolut dari Random Forest. Jaringan hierarkis ini sukses mereduksi ketidakpastian (uncertainty) spasial dari algoritma linear menjadi sebuah keputusan diskrit yang nyaris nirkesalahan.



Gambar 11. Confusion Matrix Model DNN

Keberhasilan pemetaan kuantitatif pada confusion matrix tersebut secara ekuivalen direpresentasikan ke dalam kalkulasi metrik evaluasi standar yang dipaparkan pada Tabel 2. Berdasarkan laporan komputasi komprehensif tersebut, arsitektur Stacked Ensemble berhasil membukukan skor Akurasi sebesar 99,97%, tingkat Presisi 99,96%, Sensitivitas (Recall) 99,97%, dan F1-Score sebesar 99,97%. Lonjakan metrik performa ini mengonfirmasi hipotesis fundamental dari metode ensemble, di mana DNN terbukti mampu mengeksplorasi dan menambal defisit kelemahan prediksi SVM (yang sebelumnya berada di rentang ~89%) dengan memanfaatkan tingkat keyakinan absolut dari Random Forest.

Tabel 2. Laporan Evaluasi Jaringan Saraf Tiruan (DNN)

Metrik Evaluasi	Nilai
Accuracy	0.999746835443
Precision	0.999668874172
Recall	0.999795165916
F1-Score	0.999731944221

3.3 Pembahasan

Pencapaian tingkat akurasi sebesar 99,97% pada arsitektur Hybrid Stacked Ensemble yang diusulkan mengonfirmasi bahwa integrasi hierarkis antara algoritma klasifikasi dasar dan jaringan saraf tiruan mampu secara efektif memecahkan tantangan deteksi anomali pada Software-Defined Networking (SDN). Keberhasilan arsitektur ini secara fundamental bermula dari keputusan reduksi dimensi yang sangat agresif, di mana sistem hanya mengandalkan lima fitur prioritas yang merepresentasikan 71,9% varians informasi dataset. Walaupun pemangkasan ekstrem ini menyebabkan degradasi performa Support Vector Machine (SVM) ke level 92,13%, kelemahan individual tersebut justru menjadi katalis matematis yang krusial bagi arsitektur ensemble. Penurunan korelasi prediksi antara Random Forest dan SVM menjadi 0,86 memaksa model Deep Neural Network (DNN) di Level 1 untuk bekerja lebih keras dalam mengekstrak pola probabilitas yang beraneka ragam (predictive diversity). Dinamika kognitif ini berhasil menghindarkan sistem dari jebakan overfitting buta, di mana DNN membuktikan kapasitasnya dalam menambal ketidakpastian komputasional SVM menggunakan landasan keyakinan Random Forest.

Secara operasional dalam ekosistem jaringan SDN, keunggulan arsitektur ini tidak sekadar diukur dari keberhasilan menembus metrik global yang tinggi, melainkan dari presisi deteksi ancamannya yang mencatatkan nihil kelolosan (zero False Negative). Di sisi lain, sistem gabungan ini hanya menghasilkan lima insiden False Positive dari 19.750 sampel pengujian. Tingkat alarm palsu (False Alarm Rate) yang sangat marginal ini memberikan garansi arsitektural bahwa mekanisme inspeksi keamanan yang diterapkan tidak akan mengintervensi atau merusak kualitas layanan (QoS) akibat pemblokiran lalu lintas pengguna sah secara sembarangan.

Skor evaluasi yang nyaris menyentuh kesempurnaan sering kali memicu keraguan akademik bahwa model sekadar menghafal pola statis atau artefak spesifik dari dataset (dataset-specific artifact). Namun, akurasi masif tersebut dipertanggungjawabkan melalui karakteristik intrinsik fitur eksklusif hasil seleksi—seperti byteperflow, pktrate, pktperflow, pktcount, dan bytecount—yang memang menyimpan jarak margin numerik ekstrem antara lalu lintas wajar dan banjir paket serangan DDoS volumetrik, serta diperkuat oleh isolasi standardisasi data latih dan skema validasi silang Out-of-Fold (OOF) untuk mengeliminasi kebocoran data (data leakage). Lebih lanjut, menanggapi keharusan analisis trade-off durasi komputasi (latency) sebagai prasyarat kelayakan pada Software-Defined Networking (SDN), arsitektur bertingkat ini dirancang dengan kompleksitas yang dikendalikan melalui reduksi dimensi masif (hanya 5 fitur). Meskipun penambahan lapisan meta-learner di Level 1 menghadirkan overhead komputasi tambahan dibanding model tunggal, pemangkasan ruang fitur yang agresif secara teoretis berhasil mereduksi beban komputasi secara signifikan pada tahap ekstraksi, sehingga waktu tunda pemrosesan keseluruhan tetap berada dalam batas toleransi operasional kontroler SDN tanpa mengorbankan kualitas layanan (QoS).

Guna memperkuat validasi metodologis serta mengonfirmasi posisi kontribusi penelitian ini terhadap lanskap ilmiah yang ada, hasil kinerja arsitektur yang diusulkan dibandingkan secara langsung dengan beberapa penelitian terdahulu pada domain deteksi keamanan SDN dan IoT. Berdasarkan hasil kajian komparatif, model single maupun hybrid berbasis ML dan DL yang diuji pada penelitian [17] menggunakan dataset ASEADOS-SDN-IoT hanya mencatatkan nilai ROC-AUC pada rentang 96%–99%. Penelitian [4] yang menggabungkan ML, DL, dan interpretabilitas SHAP pada dataset SDN-ATK, serta penelitian [9] yang mengandalkan AutoML TPOT dengan optimasi genetika pada dataset KDD Cup 99 dan SDN-DDoS, masing-masing hanya mampu memperoleh metrik evaluasi di kisaran 98%–99% dan akurasi 99,00%. Sementara itu, pendekatan Convolutional Neural Network (CNN) oleh [6] menghasilkan akurasi 97,74% pada dataset InSDN dan 99,90% pada CTU-13. Pada skenario serangan spesifik, penelitian [2] menunjukkan efektivitas pemodelan probabilistik mstate khusus untuk Slow-Rate DDoS, sedangkan penelitian [14] memanfaatkan Deep Transfer Learning (BiLSTM dan CNN) pada dataset 5G-NIDD untuk meningkatkan F1-Score hingga 10%. Jika dibandingkan dengan pengujian baseline internal menggunakan Single DNN Model pada dataset SDN DDoS yang sama (Akurasi 99,77% dan Recall 99,73%), arsitektur Stacked Ensemble (RF + SVM → DNN) yang diusulkan terbukti lebih unggul dengan meraih Akurasi sebesar 99,97% dan Recall 100,00%..

Melalui integrasi komparatif tersebut, posisi keunggulan arsitektur hibrida ini dikukuhkan oleh beberapa aspek utama. Pertama, dari segi presisi dan akurasi umum, metode yang diusulkan berhasil menembus Akurasi sebesar 99,97%, mengungguli capaian model single/hybrid pada penelitian [6] sebesar 97,74%, [9] sebesar 99,00%, serta [4] yang berada pada kisaran 98%–99%. Kedua, sistem mencatatkan tingkat Recall sempurna sebesar 100,00% (zero False Negative), yang mengeliminasi potensi kelolosan paket serangan ke dalam kontroler SDN. Ketiga, dari sisi efisiensi komputasi, pendekatan seperti [4], [6] masih mengandalkan representasi fitur berdimensi tinggi atau pemrosesan kompleks berbasis CNN dan SHAP, sedangkan metode usulan membuktikan



bahwa pengolahan 5 fitur prioritas utama (byteperflow, pktrate, pktcount, duration_sec, dan pairflow) sudah sangat memadai untuk mencapai performa puncak sekaligus meminimalkan beban ekstraksi pada kontroler. Keempat, dibandingkan dengan penerapan single model pada penelitian [17] maupun baseline internal, penggabungan Random Forest dan SVM sebagai penyedia meta-features probabilistik terbukti menciptakan sinergi arsitektur berlapis yang menghasilkan representasi pola data yang jauh lebih kaya, stabil, dan andal bagi meta-learner DNN.

4. KESIMPULAN

Penelitian ini berhasil mengimplementasikan kerangka kerja deteksi intrusi untuk lingkungan Software-Defined Networking (SDN) melalui arsitektur Stacked Ensemble Learning dua tingkat yang mengintegrasikan Random Forest (RF) dan Support Vector Machine (SVM) sebagai base learners, serta Deep Neural Network (DNN) sebagai meta-learner. Penerapan seleksi fitur berbasis Gini Importance terbukti memegang peranan krusial dengan mengekstraksi lima atribut teratas yang mencakup 71,9% varians informasi, sehingga sukses mengeliminasi redundansi beban komputasi secara masif pada tahap awal. Pemotongan fitur ini berimbas pada penurunan akurasi algoritma linier SVM menjadi 92,13%, namun kondisi tersebut secara paradoks justru menciptakan keberagaman persepsi prediksi (predictive diversity) yang memberikan masukan probabilistik bervariasi bagi model tingkat lanjut. Melalui mekanisme validasi silang (cross-validation), fitur probabilistik ini secara efektif menjembatani model tingkat dasar sehingga memfasilitasi DNN untuk merumuskan keputusan klasifikasi akhir dengan capaian metrik evaluasi yang teramat superior, yakni Akurasi, Presisi, Recall, dan F1-Score sebesar 99,97%, serta luasan kurva ROC-AUC mencapai 0,99999976. Meskipun capaian ini secara empiris membuktikan keandalan sistem dalam mendeteksi serangan Distributed Denial of Service (DDoS) volumetrik, angka yang nyaris sempurna pada pengujian dataset statis menuntut kewaspadaan akademis terhadap potensi model yang sekadar menghafal karakteristik data (overfitting) alih-alih mempelajari pola generalisasi yang sesungguhnya. Oleh karena itu, guna menyempurnakan arsitektur ini, penelitian selanjutnya mutlak dituntut untuk mengukur latensi pemrosesan ujung-ke-ujung (end-to-end processing time) agar overhead komputasi dari penggabungan tiga algoritma hierarkis ini terbukti tidak memicu perlambatan kinerja (bottleneck) pada controller SDN di dunia nyata. Selain itu, tahapan evaluasi harus segera beralih dari lingkungan analitik statis menuju integrasi pengujian waktu nyata (real-time) menggunakan emulator jaringan interaktif seperti Mininet yang dikendalikan oleh controller Ryu atau POX. Sebagai tahap pengujian puncak terhadap validitas dan ketajaman batas keputusan matematis model, ketangguhan meta-learner ini juga harus dievaluasi secara ketat terhadap ancaman tingkat lanjut seperti Low-Rate DDoS maupun varian Zero-Day, yang secara spesifik dirancang untuk menyembunyikan diri dan mengeksploitasi sistem dengan cara menyerupai rutinitas lalu lintas jaringan pengguna yang wajar.

5. PERNYATAAN PENULIS

5.1. Kontribusi Penulis

Konseptualisasi: Dicopran Sisco, dan Edi Surya Negara;
Metodologi: Dicopran Sisco, dan Edi Surya Negara;
Perangkat Lunak: Dicopran Sisco, dan Edi Surya Negara;
Validasi: Dicopran Sisco, dan Edi Surya Negara;
Analisis Formal: Dicopran Sisco, dan Edi Surya Negara;
Investigasi: Dicopran Sisco, dan Edi Surya Negara;
Sumber Daya: Dicopran Sisco, dan Edi Surya Negara;
Kurasi Data: Dicopran Sisco, dan Edi Surya Negara;
Penulisan Draf Awal: Dicopran Sisco, dan Edi Surya Negara;
Penulisan, Peninjauan, dan Penyuntingan: Dicopran Sisco, dan Edi Surya Negara;
Visualisasi: Dicopran Sisco, dan Edi Surya Negara;
Seluruh penulis telah membaca dan menyetujui versi manuskrip yang telah diterbitkan.

5.2. Ketersediaan Data

Data yang disajikan dalam penelitian ini tersedia berdasarkan permintaan kepada penulis korespondensi.

5.3 Pendanaan

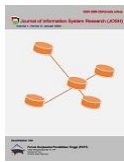
Penelitian dan penulisan manuskrip ini tidak menerima pendanaan khusus dari lembaga pemerintah, organisasi komersial, maupun organisasi nirlaba. Seluruh kegiatan penelitian dilakukan menggunakan sumber daya yang tersedia bagi penulis.

5.4 Pernyataan Dewan Peninjau Institusional

Tidak Berlaku (Not applicable).

5.5 Pernyataan Persetujuan Berdasarkan Informasi





Tidak Berlaku (Not applicable).

5.6 Pernyataan Konflik Kepentingan

Para penulis menyatakan bahwa mereka tidak memiliki kepentingan keuangan yang bersaing atau hubungan pribadi yang diketahui yang dapat dianggap memengaruhi pekerjaan yang dilaporkan dalam artikel ini.

5.7 Penggunaan AI Generatif dan Teknologi Berbantuan AI dalam Proses Penulisan

Para penulis menggunakan AI Generatif untuk meningkatkan kejelasan penulisan dalam artikel ini. Para penulis telah meninjau dan menyunting konten yang dihasilkan dengan bantuan AI serta bertanggung jawab penuh atas versi akhir publikasi.

REFERENCES

- [1] A. A. Wabi, I. Idris, O. M. Olaniyi, and J. A. Ojeniyi, "DDoS attack detection in SDN: Method of attacks, detection techniques, challenges and research gaps," *Comput. Secur.*, vol. 139, Apr. 2024, doi: 10.1016/j.cose.2023.103652.
- [2] N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz, E. Jacob, and C. Martinez-Cagnazzo, "Physical Assessment of an SDN-Based Security Framework for DDoS Attack Mitigation: Introducing the SDN-SlowRate-DDoS Dataset," *IEEE Access*, vol. 11, pp. 46820–46831, 2023, doi: 10.1109/ACCESS.2023.3274577.
- [3] M. S. Elsayed, N. A. Le-Khac, and A. D. Jurcut, "InSDN: A novel SDN intrusion dataset," *IEEE Access*, vol. 8, pp. 165263–165284, 2020, doi: 10.1109/ACCESS.2020.3022633.
- [4] S. M. Doğan, K. E. Arikan, and M. Alkan, "SDN-ATK: a novel SDN-specific attack dataset," *PeerJ Comput. Sci.*, vol. 12, 2026, doi: 10.7717/peerj-cs.3556.
- [5] K. S. Sahoo et al., "An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020, doi: 10.1109/ACCESS.2020.3009733.
- [6] U. B. Clinton, N. Hoque, and K. Robindro Singh, "Classification of DDoS attack traffic on SDN network environment using deep learning," *Cybersecurity*, vol. 7, no. 1, Dec. 2024, doi: 10.1186/S42400-024-00219-7.
- [7] H. RAHMAN and T. Sutabri, "Analysis DDoS Attack Using Machine Learning On Software-Defined Network Architectures," *JSAI (Journal Scientific and Applied Informatics)*, vol. 7, no. 3, pp. 531–536, Nov. 2024, doi: 10.36085/JSAI.V7I3.7301.
- [8] O. Polat et al., "Supervised and deep learning techniques for DDoS detection in software-defined network architectures: a systematic review," Mar. 01, 2026, Elsevier B.V. doi: 10.1016/j.jestch.2026.102290.
- [9] F. Talpur, I. A. Korejo, A. A. Chandio, A. Ghulam, and M. S. H. Talpur, "ML-Based Detection of DDoS Attacks Using Evolutionary Algorithms Optimization," *Sensors*, vol. 24, no. 5, Mar. 2024, doi: 10.3390/s24051672.
- [10] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS Detection using Deep Learning," *Procedia Comput. Sci.*, vol. 218, pp. 2420–2429, 2022, doi: 10.1016/j.procs.2023.01.217.
- [11] M. W. Nadeem, H. G. Goh, V. Ponnusamy, and Y. Aun, "DDoS Detection in SDN using Machine Learning Techniques," *Computers, Materials & Continua*, vol. 71, no. 1, pp. 771–789, Nov. 2021, doi: 10.32604/CMC.2022.021669.
- [12] A. Sanmorino, L. Marnisah, and H. Di Kesuma, "Detection of DDoS Attacks using Fine-Tuned Multi-Layer Perceptron Models," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16444–16449, Oct. 2024, doi: 10.48084/ETASR.8362.
- [13] P. Org, K. Sharma, and C. Jacobik, "Graph Neural Network-Based DDoS Protection for Data Center Infrastructure," *Pacific Northwest Software Quality Conference*, vol. 2025, pp. 293–307, Mar. 2025, doi: <https://doi.org/10.48550/arXiv.2603.13694>.
- [14] K. Noor, A. L. Imoize, C. T. Li, and C. Y. Weng, "A Review of Machine Learning and Transfer Learning Strategies for Intrusion Detection Systems in 5G and Beyond," Apr. 01, 2025, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/math13071088.
- [15] W. Hill et al., "DDoS in SDN: a review of open datasets, attack vectors and mitigation strategies," *Discover Applied Sciences*, vol. 6, no. 9, Sep. 2024, doi: 10.1007/S42452-024-06172-X.
- [16] J. S. Aguilar-Ruiz and M. Michalak, "Classification performance assessment for imbalanced multiclass data," *Sci. Rep.*, vol. 14, no. 1, p. 10759, Dec. 2024, doi: 10.1038/S41598-024-61365-Z.
- [17] T. Lakshan Yasarathna and N. A. Le-Khac, "ASEADOS-SDN-IoT: A novel SDN-IoT network intrusion detection dataset and framework," *Internet of Things (The Netherlands)*, vol. 36, Mar. 2026, doi: 10.1016/j.iot.2026.101891.
- [18] F. Ferdiansyah, D. Antoni, M. Valdo, M. Mikko, C. Mukmin, and U. Ependi, "Machine Learning Models for DDoS Detection in Software-Defined Networking: A Comparative Analysis," *Journal of Information Systems and Informatics*, vol. 6, no. 3, pp. 1790–1803, Sep. 2024, doi: 10.51519/JOURNALISI.V6I3.864.
- [19] 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," Nov. 01, 2025, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/electronics14214222.
- [20] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDOS attack detection in software defined networking," *Journal of Network and Computer Applications*, vol. 187, p. 103108, Aug. 2021, doi: 10.1016/J.JNCA.2021.103108.