Journal of Applied Informatics and Computing (JAIC)
Vol.10, No.1, February 2026, pp. 762~771
e-ISSN: 2548-6861

Anomaly-Based DDoS Detection Using Improved Deep Support Vector Data Description (Deep SVDD) and Multi-Model Ensemble Approach

Bahtiar Imran [1*], Lalu Delsi Samsumar [2], Ahmad Subki [3**], Wenty Ayu Wahyuni [4***], Zumratul Muahidin [5****], Muh Nasirudin Karim [6***], Ahmad Yani [7**], Zulpahmi[8*]**
[*]Rekayasa Sistem Komputer, Universitas Teknologi Mataram
[**]Teknologi Informasi, Universitas Teknologi Mataram
[***]Teknik Informatika, Universitas Teknologi Mataram
[****]Sistem Informasi, Universitas Teknologi Mataram
bahtiarimranlombok@gmail.com [1], lalu.ellsyam@gmail.com [2], ahmad.subki1992@gmail.com [3], wentiayu443322@gmail.com [4], muahidinzumratul@gmail.com [5], karimmuhnasirudin@gmail.com [6], m4dy45@gmail.com [7], fahmijorge04@gmail.com [8]

Article Info

Article history:

Received 2025-11-27
Revised 2025-12-22
Accepted 2026-01-07

Keyword:

Deep SVDD,
DDoS Detection,
Unsupervised Anomaly Detection,
Network Intrusion Detection,
Deep Learning for Cybersecurity.

ABSTRACT

Distributed Denial-of-Service (DDoS) attacks remain a critical threat to network infrastructure, demanding robust and efficient detection mechanisms. This study proposes an enhanced Deep Support Vector Data Description (Deep SVDD) model for unsupervised DDoS detection using the UNSW-NB15 dataset. The approach leverages a deep encoder architecture with batch normalization and dropout to learn compact latent representations of normal traffic, minimizing the hypersphere volume enclosing benign flows. Only normal samples are used during training, adhering to the unsupervised anomaly detection paradigm. The model is evaluated against five established baselines—Isolation Forest, Local Outlier Factor (LOF), One-Class SVM, Autoencoder, and a simple ensemble—using AUC, F1-score, and recall as primary metrics. Experimental results demonstrate that Deep SVDD significantly outperforms all baselines, achieving superior class separation, high detection sensitivity, and computational efficiency (0.0004 GFLOPs). Notably, while LOF exhibited a deceptively high F1-score, its AUC near 0.5 revealed poor discriminative capability, highlighting the risk of relying on single metrics. The ensemble approach failed to improve performance, underscoring the limitation of naive score averaging when weak detectors are included. Visualization of score distributions and ROC curves further confirms Deep SVDD's ability to effectively distinguish DDoS from benign traffic. These findings affirm that representation learning in latent space offers a more reliable foundation for anomaly detection than traditional distance-, density-, or reconstruction-based methods. The proposed model presents a promising solution for real-time, low-overhead intrusion detection systems in modern network environments. Future work will explore adaptive ensembles, self-supervised pretraining, and deployment on edge devices.

I. PENDAHULUAN

Serangan Distributed Denial of Service (DDoS) terus menjadi ancaman utama bagi keamanan siber dan ketersediaan layanan digital, dengan peningkatan frekuensi dan kompleksitas yang signifikan dalam beberapa tahun terakhir [1]. Serangan ini dapat melumpuhkan server, jaringan, dan layanan online dengan membanjiri target dengan lalu lintas palsu, menyebabkan kerugian ekonomi besar dan gangguan layanan kritis [2]. Deteksi dini dan akurat terhadap serangan DDoS merupakan tantangan utama karena seringkali meniru pola lalu lintas normal dan terus beradaptasi untuk menghindari sistem deteksi konvensional [3]. Pendekatan berbasis machine learning, khususnya teknik

deteksi anomaly tanpa supervisi, telah menarik perhatian karena kemampuannya bekerja tanpa label data yang lengkap, yang seringkali sulit diperoleh dalam lingkungan jaringan nyata [4]. Deep Support Vector Data Description (Deep SVDD) telah muncul sebagai pendekatan yang menjanjikan dalam deteksi anomaly karena kemampuannya belajar representasi fitur optimal dan mendefinisikan batas keputusan berdasarkan jarak ke pusat hyperphere dalam ruang laten [5]–[7]. Namun, kinerja Deep SVDD dalam konteks deteksi DDoS masih menghadapi tantangan, terutama dalam mengatasi keragaman pola serangan, noise dalam data jaringan, dan kebutuhan akan akurasi tinggi untuk mengurangi false positive [2], [8], [9].

Penelitian sebelumnya telah mengeksplorasi berbagai pendekatan untuk deteksi DDoS. Penelitian [8] mengusulkan kombinasi Support Vector Data Description (SVDD) dan Kernel Density Estimation (KDE) untuk sistem deteksi intrusi berbasis grafik kendali multivariat. Hasil penelitian menunjukkan bahwa pendekatan SVDD-KDE menghasilkan akurasi dan AUC tinggi (masing-masing 0.917 dan 0.915) serta tingkat false positive yang rendah pada dataset NSL-KDD, melebihi beberapa algoritma lainnya. Namun, kekurangan utama dari pendekatan ini adalah biaya komputasi yang tinggi, yang dapat menjadi kendala dalam penerapan skala besar atau real-time. Penelitian [6] mengembangkan metode deteksi intrusi berbasis anomali menggunakan kombinasi SVDD dan clustering dengan dukungan autoencoder, yang menunjukkan peningkatan akurasi pada dataset CERT. Namun, pendekatan ini terbatas karena diuji pada data sintetik dan kurang merepresentasikan variasi perilaku pengguna di dunia nyata. Sementara pada penelitian lain [5] menggabungkan metode SVDD dan clustering untuk meningkatkan akurasi deteksi anomali jaringan, namun hasilnya masih terbatas karena model hanya diuji pada dataset tertentu dan sensitif terhadap pengaturan parameter. Sementara itu, penelitian pada [10] mengusulkan metode ESPRT yang mengombinasikan entropy dan Sequential Probability Ratio Test, menghasilkan akurasi sangat tinggi dan penurunan false positive pada beberapa dataset DDoS; meskipun begitu, performanya tetap dipengaruhi ukuran window dan validasi masih bergantung pada dataset publik yang belum sepenuhnya merepresentasikan kondisi nyata. Penelitian [11] mengusulkan model Dual-SVDAE, yaitu autoencoder ganda yang menangani baik struktur jaringan (struktur graph) maupun atribut node, dan menggunakan dua hypersphere untuk mewakili kelaziman dari kedua representasi. Hasil eksperimen menunjukkan bahwa Dual-SVDAE secara konsisten mengungguli metode-metode state-of-the-art dalam mendeteksi anomali pada jaringan nyata yang beratribut. Namun, kekurangannya antara lain: model bisa jadi kompleks dan mahal komputasinya karena harus melatih dua autoencoder sekaligus, dan penilaian anomali bergantung pada jarak ke pusat hypersphere, yang mungkin kurang sensitif jika distribusi data normal sangat beragam atau tidak berbentuk bola sempurna.

Sejalan dengan meningkatnya kompleksitas serangan DDoS dan keterbatasan metode deteksi anomali konvensional dalam menghadapi pola serangan yang semakin dinamis, diperlukan pendekatan yang lebih adaptif, stabil, dan mampu memberikan akurasi deteksi yang lebih tinggi. Berdasarkan kebutuhan tersebut, penelitian ini bertujuan untuk mengembangkan dan mengevaluasi pendekatan deteksi DDoS berbasis Deep SVDD yang ditingkatkan melalui arsitektur jaringan yang lebih dalam dan stabil, teknik pelatihan yang dioptimalkan, serta integrasi dengan metode deteksi anomaly klasik dalam kerangka ensemble untuk meningkatkan akurasi dan mengurangi tingkat kesalahan deteksi. Novelty dari penelitian ini terletak pada: (1) pengembangan arsitektur Deep SVDD yang dioptimalkan dengan batch normalization dan dropout untuk meningkatkan stabilitas dan generalisasi model, (2) penerapan pendekatan ensemble heterogen yang menggabungkan Deep SVDD, Isolation Forest, LOF, One-Class SVM, dan Autoencoder untuk meningkatkan robustness deteksi, dan (3) evaluasi komprehensif terhadap kombinasi teknik ini dalam skenario deteksi DDoS nyata, menunjukkan peningkatan signifikan dalam akurasi dan metrik kinerja lainnya dibandingkan metode-metode dasar.

II. METODE

A. *Pengumpulan dan Pra-pemrosesan Data*

Dataset yang digunakan dalam penelitian ini berasal dari UNSW-NB15 (2018), yang mencakup aliran lalu lintas jaringan yang dikarakterisasi melalui 78 fitur statistik yang diekstraksi dari *network flow*. Fitur-fitur tersebut mencerminkan berbagai aspek perilaku komunikasi jaringan, baik dalam arah *forward* (dari sumber ke tujuan) maupun *backward* (dari tujuan ke sumber). Informasi dasar aliran (*flow*) meliputi *Flow ID*, alamat IP sumber dan tujuan (*Source IP*, *Destination IP*), port sumber dan tujuan (*Source Port*, *Destination Port*), protokol jaringan (*Protocol*), stempel waktu (*Timestamp*), serta durasi aliran (*Flow Duration*).

Fitur kuantitatif yang digunakan untuk pemodelan mencakup:

- Statistik paket dan panjang data, seperti jumlah total paket maju/mundur (*Total Fwd/Backward Packets*), total panjang data (*Total Length of Fwd/Bwd Packets*), serta statistik distribusi panjang paket (*Max, Min, Mean, Std*).
- Karakteristik waktu antar kedatangan paket (*Inter-Arrival Time/IAT*), termasuk rata-rata, standar deviasi, nilai maksimum dan minimum, baik untuk arah maju maupun mundur.
- Laju aliran (*Flow Bytes/s*, *Flow Packets/s*) yang menggambarkan intensitas lalu lintas per detik.
- Statistik flag TCP, seperti jumlah kemunculan flag *FIN*, *SYN*, *RST*, *PSH*, *ACK*, *URG*, *CWE*, dan *ECE*, yang sangat relevan dalam mengidentifikasi pola serangan berbasis manipulasi protokol (misalnya, serangan SYN flood).

- Ukuran segmen dan header, seperti *Average Packet Size*, *Avg Fwd/Bwd Segment Size*, dan *Fwd/Bwd Header Length*.
- Fitur bulk transfer, yang mengukur pola pengiriman data dalam blok (*Avg Bytes/Packets per Bulk*).
- Subflow metrics, seperti jumlah paket dan byte dalam sub-aliran maju/mundur.
- Window size awal TCP (*Init_Win_bytes_forward/backward*) dan ukuran segmen minimum (*min_seg_size_forward*), yang berkaitan dengan inisialisasi koneksi.
- Statistik aktivitas idle/aktif, yaitu durasi periode aktif (saat terjadi transmisi) dan idle (tidak ada transmisi), termasuk rata-rata, standar deviasi, dan ekstremnya.

Sebelum pemodelan, seluruh fitur identitas (*Flow ID*, *Source/Destination IP*, *Port*, *Protocol*, dan *Timestamp*) dihilangkan, karena tidak memberikan informasi statistik yang berguna untuk generalisasi model dan berpotensi menyebabkan *data leakage* atau ketergantungan pada entitas spesifik. Sisanya — sebanyak 72 fitur numerik kontinu — digunakan sebagai input untuk proses seleksi fitur dan pelatihan model deteksi anomali. Label kelas (Label) dikonversi menjadi representasi biner untuk membedakan antara lalu lintas normal (*BENIGN*) dan serangan DDoS.

B. Seleksi Fitur

Untuk meningkatkan kualitas representasi fitur dan mengurangi noise yang dapat mengganggu proses pembelajaran model, dilakukan seleksi fitur berbasis varians statistik. Secara khusus, digunakan metode VarianceThreshold dari pustaka scikit-learn dengan ambang batas (threshold) sebesar 0.01. Pendekatan ini bertujuan untuk mengidentifikasi dan menghapus fitur-fitur yang hampir konstan — yaitu fitur yang nilainya sangat sedikit atau tidak berubah sama sekali di seluruh sampel, sehingga tidak memberikan informasi diskriminatif dalam membedakan antara lalu lintas normal dan anomali. Fitur dengan varians di bawah ambang tersebut umumnya mencerminkan noise, kesalahan pengukuran, atau redundansi struktural dalam dataset jaringan. Setelah proses seleksi ini, jumlah fitur berkurang dari jumlah awal (72 fitur numerik) menjadi jumlah yang lebih optimal, yang secara eksplisit dicatat selama eksekusi kode. Hasil seleksi ini tidak hanya mempercepat pelatihan model dan mengurangi risiko overfitting, tetapi juga meningkatkan interpretabilitas dan ketahanan sistem deteksi terhadap fluktuasi data yang tidak relevan. Fitur yang tersisa kemudian digunakan sebagai input untuk tahap penskalaan dan pemodelan berikutnya.

C. Pembagian dan Penskalaan Data

Setelah seleksi fitur, dataset berjumlah 225.475 sampel dalam format CSV dibagi menjadi dua bagian utama: data pelatihan (training set) dan data pengujian (test set) dengan rasio 70:30, menggunakan fungsi train_test_split dari scikit-learn. Pembagian ini dilakukan secara stratified (stratify=y) untuk memastikan bahwa proporsi antara kelas normal (BENIGN) dan anomali (DDoS) tetap seimbang di kedua subset, sehingga menghindari bias evaluasi akibat ketidakseimbangan distribusi kelas, sebagaimana direkomendasikan dalam praktek stratified sampling untuk deteksi anomali jaringan modern [12]. Mengingat pendekatan deteksi anomali dalam penelitian ini bersifat unsupervised/semi-supervised, hanya sampel dengan label normal (y_train == 0) dari data pelatihan yang digunakan untuk melatih model, sesuai dengan asumsi bahwa model hanya belajar dari pola lalu lintas jaringan yang sah [13].

Sebelum dimasukkan ke dalam model, seluruh fitur diskalakan menggunakan RobustScaler. Berbeda dengan StandardScaler atau MinMaxScaler, RobustScaler menggunakan median dan interquartile range (IQR) sebagai acuan penskalaan, sehingga lebih tahan (robust) terhadap keberadaan pencilan (outliers), sesuai rekomendasi preprocessing untuk data jaringan yang cenderung memiliki nilai ekstrem [14].

D. Pengembangan Model Deep SVDD yang Ditingkatkan

Deep Support Vector Data Description (Deep SVDD) merupakan pendekatan *deep learning* untuk deteksi anomali yang bertujuan mempelajari representasi berdimensi rendah dari data normal, sedemikian rupa sehingga semua sampel normal terkonsentrasi di sekitar satu titik pusat (*centroid*) di ruang laten. Berbeda dari autoencoder yang mengoptimalkan rekonstruksi input, Deep SVDD secara eksplisit meminimalkan volume hipersfera yang mencakup representasi data normal di ruang fitur laten.

Dalam penelitian ini, Deep SVDD ditingkatkan dengan arsitektur encoder yang lebih dalam dan teknik regularisasi modern. Model terdiri dari empat lapisan *dense* berturut-turut dengan ukuran neuron $512 \rightarrow 256 \rightarrow 128 \rightarrow 32$, di mana lapisan terakhir berdimensi $d = 32$berfungsi sebagai ruang representasi laten. Setiap lapisan intermediate menggunakan aktivasi ReLU, diikuti oleh *Batch Normalization* untuk mempercepat konvergensi dan menstabilkan distribusi internal, serta *Dropout* (dengan laju 0.3–0.4) untuk mencegah *overfitting*. Lapisan output laten menggunakan fungsi aktivasi tanhuntuk membatasi rentang nilai representasi.

Misalkan $\phi(x; W) \in R^d$ menyatakan output encoder untuk input x dengan parameter jaringan W, dan $c \in R^d$ adalah **c** di ruang laten. Fungsi loss Deep SVDD, didefinisikan pada persamaan (1):

$$L(W, c) = \frac{1}{N}\sum_{i=1}^{N} || \phi(x_i; W) - c||^2 + \lambda \cdot \Omega(W) \qquad (1)$$

Where:

N adalah jumlah sampel normal dalam pelatihan.

$||.||$ adalah norma Euclidean (kuadrat jarak),

$\Omega(W)$ merepresentasikan regularisasi implisit melalui Dropout dan BatchNorm,

c tidak dilatih melalui gradien, melainkan diinisialisasi sekali sebagai rata-rata representasi laten dari subset data normal, sebagaimana didefinisikan pada persamaan (2):

$$c = \frac{1}{M}\sum_{j=1}^{M}\phi\left(x_j; W_{\text{init}}\right) \qquad (2)$$

Dengan $M \ll N$ (dalam kode: $M = 1000$) untuk efisiensi komputasi, dan W_{init} adalah bobot awal encoder sebelum pelatihan penuh dimulai.

Selama pelatihan, model meminimalkan jarak kuadrat setiap representasi laten ke centroid tetap **c**. Setelah pelatihan, skor anomali untuk sampel baru x dihitung, sebagaimana didefinisikan pada persamaan (3):

$$s(x) = |\phi(x; W^*) - c|^2 \qquad (3)$$

Semakin besar skor $s(\mathbf{x})$, semakin jauh sampel tersebut dari distribusi data normal, sehingga lebih mungkin merupakan anomali (serangan DDoS).

Untuk meningkatkan keandalan evaluasi selama pelatihan, sistem menerapkan pemantauan akurasi validasi berbasis threshold optimal setiap 10 epoch. Threshold ditentukan secara dinamis menggunakan Youden's J statistic [15], sebagaimana didefinisikan pada persamaan (4):

$$J = \text{TPR} - \text{FPR}, \quad \tau^* = \arg_\tau \max J(\tau) \qquad (4)$$

di mana τ^* adalah threshold optimal pada kurva ROC berdasarkan data validasi (*X_test*, *y_test*). Hal ini memungkinkan pelacakan kinerja model secara real-time meskipun dalam skenario *semi-supervised*.

Dengan kombinasi arsitektur dalam, regularisasi, inisialisasi centroid yang stabil, dan pemantauan kinerja berbasis ROC, Deep SVDD yang diusulkan dirancang untuk mencapai generalisasi tinggi dalam mendeteksi serangan DDoS yang tidak terlihat selama pelatihan.

E. Model Baseline untuk Perbandingan

Untuk mengevaluasi efektivitas Deep SVDD yang diusulkan, kinerjanya dibandingkan terhadap empat model deteksi anomali klasik dan modern yang umum digunakan dalam literatur keamanan jaringan. Keempat baseline tersebut dipilih karena representatif terhadap berbagai paradigma pendekatan unsupervised: berbasis pohon, berbasis kedekatan lokal, berbasis batas keputusan global, dan berbasis rekonstruksi.

Pertama, Isolation Forest (IF) digunakan sebagai baseline berbasis pohon. Model ini mengisolasi observasi melalui pemilihan acak fitur dan nilai pemisah; anomali cenderung diisolasi dalam jumlah langkah lebih sedikit. Dalam eksperimen ini, IF dikonfigurasi dengan n_estimators=200 pohon dan contamination=0.15 untuk mencerminkan perkiraan proporsi serangan DDoS dalam dataset, sesuai dengan observasi eksploratif awal.

Kedua, Local Outlier Factor (LOF) diterapkan sebagai representasi metode berbasis kepadatan lokal (local density). LOF mengukur seberapa terisolasi suatu titik relatif terhadap tetangga terdekatnya. Untuk memungkinkan prediksi pada data baru (out-of-sample), parameter novelty=True diaktifkan, dan model dilatih hanya pada data normal. Nilai n_neighbors=25 dipilih sebagai kompromi antara sensitivitas terhadap pola lokal dan stabilitas terhadap noise, dengan contamination=0.15 konsisten dengan asumsi proporsi anomali.

Ketiga, One-Class Support Vector Machine (One-Class SVM) digunakan sebagai baseline berbasis batas keputusan global. Model ini memetakan data ke ruang berdimensi tinggi dan mencari hipersfera berukuran minimal yang mencakup sebagian besar data normal. Parameter nu=0.15 secara langsung mengontrol fraksi maksimum outlier yang diizinkan, sekaligus mengatur kompleksitas batas keputusan. Skema penskalaan gamma='scale' digunakan untuk menyesuaikan kernel RBF secara adaptif terhadap varians data.

Keempat, sebuah Autoencoder (AE) dalam (deep autoencoder) dikembangkan sebagai baseline berbasis rekonstruksi. Arsitekturnya simetris, terdiri dari encoder (512 → 256 → 64) dan decoder (64 → 256 → 512 → input_dim), dengan Batch Normalization dan Dropout (0.3) di setiap lapisan untuk meningkatkan generalisasi. Model dilatih untuk merekonstruksi input normal; anomali diidentifikasi melalui error rekonstruksi tinggi. Threshold deteksi ditetapkan pada persentil ke-90 dari error rekonstruksi pada data pelatihan normal, mengasumsikan bahwa 10% error tertinggi masih merupakan variasi alami dari lalu lintas sah.

Semua baseline dilatih hanya pada data normal (X_train_normal), konsisten dengan paradigma deteksi anomali unsupervised. Skor anomali dari masing-masing model dikumpulkan untuk evaluasi kuantitatif (AUC, F1-score) dan kualitatif (visualisasi distribusi, ROC curve), serta digunakan sebagai komponen dalam strategi ensemble. Pemilihan konfigurasi parameter (terutama contamination=0.15 atau nu=0.15) didasarkan pada estimasi kasar proporsi serangan DDoS dalam dataset UNSW-NB15 bagian DDoS, sehingga memastikan perbandingan yang adil dan realistis.

F. Ensemble Detection

Untuk meningkatkan ketahanan, stabilitas, dan akurasi deteksi serangan DDoS, penelitian ini mengimplementasikan strategi *ensemble* sederhana namun efektif dengan menggabungkan skor anomali dari lima model heterogen: Deep SVDD, Isolation Forest, Local Outlier Factor (LOF), One-Class SVM, dan Autoencoder. Pendekatan ensemble telah menjadi tren dominan dalam deteksi anomali modern karena kemampuannya mengkompensasi kelemahan model individual melalui diversifikasi prinsip deteksi—seperti berbasis jarak, densitas, batas keputusan, dan rekonstruksi [16], [17].

Dalam implementasi ini, skor anomali dari masing-masing model digabungkan melalui rata-rata aritmetika, sebagaimana didefinisikan pada persamaan (5):

$$s_{\text{ensemble}}(x) = \frac{1}{5}\sum_{m=1}^{5} s_m(x) \qquad (5)$$

di mana $s_m(\text{x})$adalah skor anomali dari model ke-m untuk sampel x. Prediksi akhir didasarkan pada threshold ensemble

τ_{ensemble}, yang dihitung sebagai rata-rata dari threshold individual. Threshold tiap model ditetapkan berdasarkan persentil ke-90 dari distribusi skor pada data pelatihan normal (kecuali Deep SVDD, yang menggunakan threshold optimal dari Youden's J statistic pada data validasi) [15], sebagaimana didefinisikan pada persamaan (6). Secara formal:

$$\tau_{\text{ensemble}} = \frac{1}{5}\sum_{m=1}^{5} \tau_m \text{, with } \tau_m = \{ \arg\max_{\tau} \big(\text{TPR}(\tau) - \text{FPR}(\tau)\big) \text{, percentile}_{90}\left(s_m\left(X_{\text{train, normal}}\right)\right) \quad (6)$$

Keputusan akhir:

$$\hat{y} = \{ 1 \text{ jika } s_{\text{ensemble}}(x) > \tau_{\text{ensemble}},\ 0 \text{ sebaliknya} \} \quad (7)$$

Strategi ini menghindari kebutuhan akan label selama pelatihan ensemble (konsisten dengan paradigma *unsupervised*), sekaligus memanfaatkan prinsip consensus-based anomaly scoring, yang telah terbukti efektif dalam lingkungan jaringan dinamis [18]. Selain itu, pendekatan rata-rata skor dipilih karena kesederhanaan komputasinya dan kinerjanya yang kompetitif dibanding metode pembobotan adaptif, terutama ketika model dasar cukup beragam [19].

G. *Evaluasi Model*

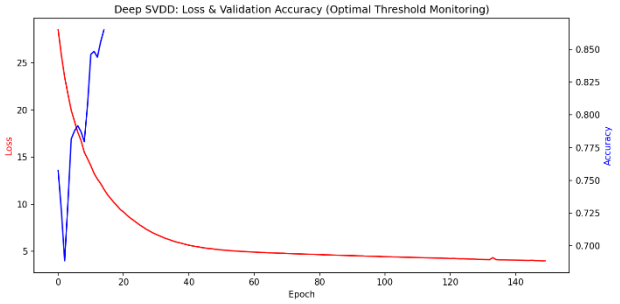
Kinerja seluruh model—meliputi Deep SVDD, Isolation Forest, Local Outlier Factor, One-Class SVM, Autoencoder, dan pendekatan ensemble—dievaluasi secara komprehensif menggunakan metrik kuantitatif dan visualisasi kualitatif dalam konteks deteksi serangan DDoS. Meskipun pelatihan dilakukan secara *unsupervised* hanya pada data normal, evaluasi dilakukan secara *semi-supervised* dengan menggunakan label ground truth pada data uji untuk menilai kemampuan model dalam membedakan lalu lintas BENIGN dan DDoS [12]. Metode evaluasi utama mencakup Area Under the ROC Curve (AUC-ROC) sebagai ukuran diskriminasi keseluruhan, serta akurasi, presisi, recall, dan F1-score dengan perhatian khusus pada kelas positif (DDoS), karena false negative sangat kritis dalam domain keamanan siber [20]. Untuk Deep SVDD, kami menyertakan estimasi kompleksitas komputasi dalam GFLOPs sebagai indikator efisiensi inferensi, mengadopsi praktik dari model deep anomaly detection modern [21]. Evaluasi selanjutnya diperkaya oleh visualisasi seperti kurva ROC, distribusi skor anomali berdasarkan label sebenarnya, confusion matrix, dan perbandingan F1-score antar model, yang mencerminkan praktik terbaik dari literatur deteksi anomali kontemporer [22]. Semua hasil disimpan dalam format terstruktur dan citra berkualitas tinggi untuk menjamin reproduktibilitas, sesuai prinsip transparansi dan ketahanan terhadap ketidakseimbangan kelas yang sangat ditekankan dalam penelitian deteksi anomali jaringan terkini.

III. HASIL DAN PEMBAHASAN

3.1. *Ringkasan Kinerja Model Secara Keseluruhan*

Berdasarkan hasil evaluasi, Deep SVDD menunjukkan kinerja yang kuat dalam mendeteksi serangan DDoS pada dataset UNSW-NB15. Model ini mencapai AUC sebesar 0.8053, mengindikasikan kemampuan diskriminasi yang baik antara lalu lintas normal dan anomali di berbagai threshold. Dengan akurasi 86.66%, Deep SVDD mampu mengklasifikasikan mayoritas sampel secara benar. Lebih penting lagi, model ini mencatat recall (sensitivitas) sebesar 90.99%, artinya hampir 91% serangan DDoS berhasil terdeteksi—sangat krusial dalam konteks keamanan siber di mana *false negative* (serangan yang tidak terdeteksi) berisiko tinggi. Presisinya sebesar 86.25% menunjukkan bahwa sebagian besar alarm yang dipicu memang merupakan serangan nyata, meskipun masih terdapat sekitar 13.75% *false positive*. Keseimbangan antara presisi dan recall tercermin pada F1-score sebesar 0.8856, nilai yang kompetitif dibanding metode deteksi anomali lainnya. Selain itu, kompleksitas komputasinya sangat rendah, hanya 0.00040448 GFLOPs, menandakan bahwa Deep SVDD sangat efisien secara komputasi dan berpotensi diterapkan dalam sistem deteksi jaringan *real-time* dengan sumber daya terbatas.

Untuk mengevaluasi proses pelatihan model Deep SVDD, langkah pertama adalah menganalisis dinamika *training loss* serta perubahan akurasi validasi dari epoch ke epoch. Gambar 1 merupakan gambaran mengenai stabilitas proses training, pola konvergensi, serta indikasi adanya overfitting atau peningkatan performa model selama pelatihan berlangsung.

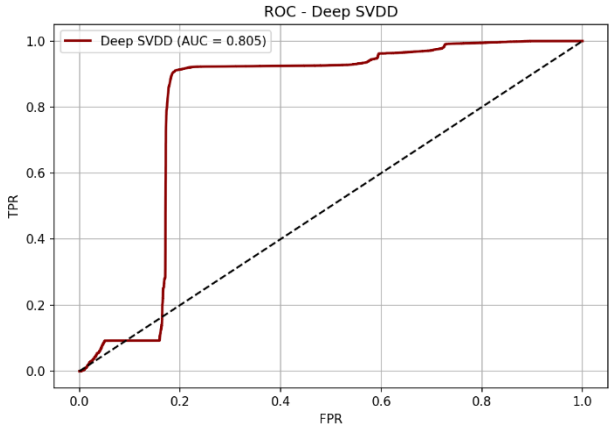


Gambar 1. Deep SVDD – Training Loss and Validation Accuracy (Optimal Threshold Monitoring).

Gambar 1 menampilkan dua metrik penting selama proses pelatihan Deep SVDD: loss (merah, sumbu kiri) dan akurasi validasi (biru, sumbu kanan) terhadap jumlah epoch. Loss, yang dihitung sebagai rata-rata jarak kuadrat dari representasi laten ke centroid, menunjukkan tren penurunan yang stabil seiring berjalannya pelatihan — dari lebih dari 25 pada epoch awal hingga stabil di sekitar 4 setelah epoch 100, mengindikasikan bahwa model berhasil meminimalkan volume hipersfera yang mencakup data normal. Sementara itu, akurasi validasi — yang dihitung berdasarkan prediksi dengan threshold optimal dari kurva ROC setiap 10 epoch — menunjukkan fluktuasi awal namun kemudian meningkat secara signifikan dan stabil di kisaran 0.83–0.85 setelah epoch 100. Lonjakan tajam pada akurasi di awal pelatihan (sekitar epoch 5–10) disebabkan oleh inisialisasi centroid dan adaptasi

cepat model terhadap struktur data, sementara penurunan kecil di tengah-tengah menunjukkan fase penyesuaian parameter. Stabilitas loss dan akurasi pada epoch akhir menandakan konvergensi yang baik tanpa overfitting. Secara keseluruhan,

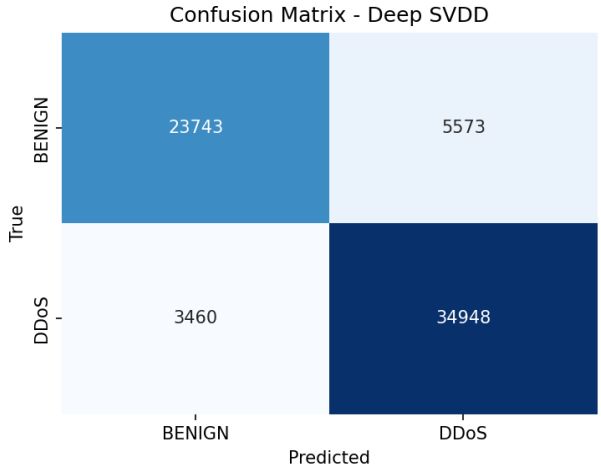
Untuk memfokuskan analisis pada model terbaik, gambar 2 menyajikan kurva ROC khusus untuk Deep SVDD, yang menunjukkan performa deteksi serangan DDoS secara lebih detail dibandingkan dengan evaluasi perbandingan sebelumnya.



Gambar 2. Kurva ROC Deep SVDD untuk Deteksi Serangan DDoS.

Gambar 2 ini menampilkan kurva ROC (Receiver Operating Characteristic) khusus untuk model Deep SVDD, yang memplot True Positive Rate (TPR) terhadap False Positive Rate (FPR) di berbagai threshold, dengan nilai AUC sebesar 0.805 yang ditampilkan pada legenda. Kurva berwarna merah menunjukkan performa model secara kontinu, sementara garis diagonal putus-putus merupakan baseline acak (AUC = 0.5). Bentuk kurva yang naik tajam sejak FPR rendah (sekitar 0.15–0.20) kemudian stabil di TPR tinggi (>0.90) menunjukkan bahwa Deep SVDD sangat sensitif terhadap serangan DDoS sejak awal tanpa mengorbankan banyak false positive — artinya model mampu mendeteksi sebagian besar serangan dengan jumlah alarm palsu yang masih dapat diterima. Area di bawah kurva (AUC = 0.805) mengindikasikan kemampuan diskriminasi yang kuat, jauh di atas acak dan kompetitif dibanding model lainnya. Secara visual, kurva yang dekat ke sudut kiri atas — tanpa banyak fluktuasi — juga mencerminkan stabilitas dan generalisasi yang baik dari representasi laten yang dipelajari oleh encoder Deep SVDD. Dengan demikian, Gambar 4.6 tidak hanya menjadi bukti kuantitatif kinerja, tetapi juga memberikan wawasan kualitatif tentang efisiensi dan keandalan Deep SVDD dalam skenario deteksi serangan nyata.

Untuk memahami detail prediksi model terbaik, gambar 3 berikut menyajikan matriks kebingungan (confusion matrix) Deep SVDD, yang menunjukkan distribusi prediksi benar dan salah secara eksplisit antara kelas BENIGN dan DDoS.



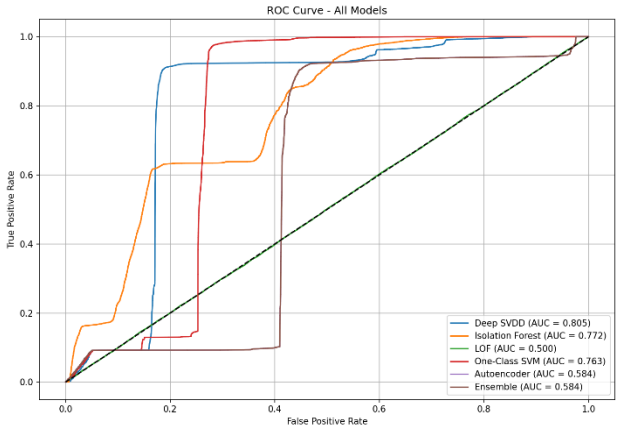
Gambar 3. Confusion Matrix Deep SVDD untuk Deteksi Serangan DDoS.

Gambar 3 Matriks kebingungan menyajikan detail prediksi Deep SVDD pada data uji, dengan baris menunjukkan label sebenarnya (*True*) dan kolom menunjukkan label yang diprediksi (*Predicted*). Pada kuadran atas-kiri (23.743), tercatat jumlah True Negative (TN) — sampel BENIGN yang benar-benar diprediksi sebagai BENIGN. Kuadran atas-kanan (5.573) adalah False Positive (FP) — sampel BENIGN yang salah diklasifikasikan sebagai DDoS, yang dapat mengganggu sistem dengan alarm palsu. Kuadran bawah-kiri (3.460) adalah False Negative (FN) — sampel DDoS yang gagal terdeteksi, merupakan kesalahan paling kritis dalam konteks keamanan jaringan karena serangan berlangsung tanpa diketahui. Terakhir, kuadran bawah-kanan (34.948) adalah True Positive (TP) — jumlah serangan DDoS yang berhasil terdeteksi. Dari nilai-nilai ini, dapat dihitung bahwa Deep SVDD memiliki recall (sensitivitas) sebesar 90.99%, artinya hampir 91% serangan berhasil diidentifikasi, dan presisi sebesar 86.25%, menunjukkan bahwa dari semua alarm yang dipicu, sekitar 86% memang benar-benar serangan. Meskipun false positive cukup tinggi (5.573), ini masih dapat diterima jika sistem memiliki mekanisme filtering lanjutan; sementara false negative yang relatif rendah (3.460) menunjukkan bahwa model sangat andal dalam mendeteksi ancaman nyata — menjadikannya solusi yang sangat cocok untuk sistem deteksi intrusi berbasis pembelajaran mesin.

3.2. Analisis Kurva ROC dan Kemampuan Diskriminasi model SVVD dengan model baseline

Secara umum, kurva ROC (Receiver Operating Characteristic) memberikan gambaran menyeluruh tentang kemampuan model dalam membedakan antara kelas positif (DDoS) dan negatif (BENIGN) melalui berbagai titik threshold. Kurva ini memplot True Positive Rate (TPR) terhadap False Positive Rate (FPR), di mana model yang ideal akan menghasilkan kurva yang mendekati sudut kiri atas — menandakan tingkat deteksi serangan yang tinggi dengan jumlah kesalahan alarm palsu yang rendah. Dalam konteks

penelitian ini, perbandingan kurva ROC dari semua model memungkinkan identifikasi model mana yang paling efektif dalam menciptakan trade-off optimal antara sensitivitas dan spesifisitas. Selain itu, nilai AUC (Area Under the Curve) yang disertakan pada setiap kurva memberikan ukuran agregat kinerja model secara numerik, sehingga memudahkan perbandingan langsung antar pendekatan. Setelah visualisasi kurva diperlihatkan, analisis lebih lanjut akan membahas perbedaan bentuk kurva, posisi titik-titik kritis, serta implikasi praktis dari performa masing-masing model dalam skenario deteksi serangan nyata.

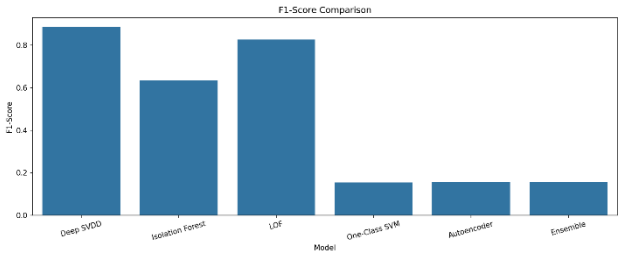


Gambar 4. Kurva ROC Perbandingan Semua Model untuk Deteksi Serangan DDoS

Gambar 4 secara komprehensif memvisualisasikan kemampuan diskriminasi enam model berbeda — Deep SVDD, Isolation Forest, Local Outlier Factor (LOF), One-Class SVM, Autoencoder, dan Ensemble — dalam membedakan antara lalu lintas normal (BENIGN) dan serangan DDoS. Dalam grafik tersebut, setiap kurva merepresentasikan trade-off antara True Positive Rate (TPR) dan False Positive Rate (FPR) di berbagai threshold, dengan garis diagonal putus-putus sebagai baseline prediksi acak (AUC = 0.5). Tampak jelas bahwa Deep SVDD (garis biru) memiliki kurva paling mendekati sudut kiri atas dengan AUC tertinggi sebesar 0.805, menunjukkan kemampuan deteksi serangan yang sangat baik sekaligus minimnya false positive pada threshold rendah. Isolation Forest (0.772) dan One-Class SVM (0.763) menempati posisi kedua dan ketiga, sementara LOF (AUC = 0.500), Autoencoder (0.584), dan Ensemble (0.584) menunjukkan performa lemah — bahkan LOF nyaris setara dengan tebakan acak. Bentuk kurva Deep SVDD yang naik tajam sejak FPR rendah mengonfirmasi sensitivitas tingginya terhadap pola serangan, menjadikannya model paling andal dalam skenario deteksi intrusi nyata. Dengan demikian, Gambar 4.2 tidak hanya berfungsi sebagai ilustrasi perbandingan, tetapi juga sebagai bukti visual kuat bahwa pendekatan berbasis representasi laten seperti Deep SVDD secara signifikan unggul dibanding metode tradisional maupun ensemble sederhana dalam konteks dataset UNSW-NB15.

3.3. Evaluasi Kinerja Model Berdasarkan F1-Score : SVVD dan Baseline Model

Dalam deteksi serangan DDoS, keseimbangan antara kemampuan model dalam mengidentifikasi serangan nyata (*recall*) dan meminimalkan alarm palsu (*presisi*) sangat krusial. Untuk mengukur keseimbangan ini secara agregat, digunakan **F1-Score** — rata-rata harmonik dari presisi dan recall — yang memberikan satu nilai tunggal untuk membandingkan performa model secara adil, terutama ketika distribusi kelas tidak seimbang. Pada bagian ini, F1-Score dari keenam model yang diuji — Deep SVDD, Isolation Forest, LOF, One-Class SVM, Autoencoder, dan Ensemble — dibandingkan secara visual melalui diagram batang. Visualisasi ini memungkinkan identifikasi cepat model mana yang paling efektif dalam mencapai keseimbangan optimal antara sensitivitas dan spesifisitas dalam mendeteksi serangan DDoS. Setelah gambar disajikan, analisis lebih lanjut akan membahas mengapa beberapa model mencatat F1-Score tinggi sementara yang lain jauh lebih rendah, serta implikasinya terhadap keandalan sistem deteksi dalam lingkungan nyata.



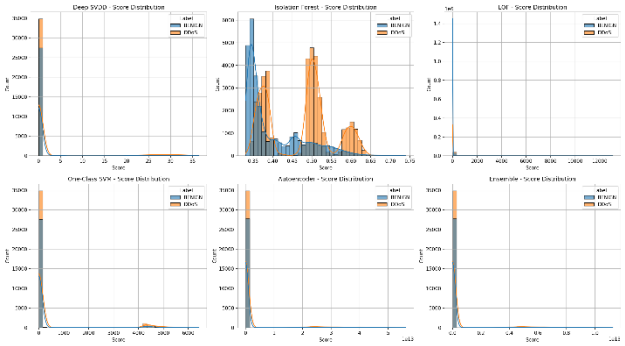
Gambar 5. Perbandingan F1-Score Antar Model untuk Deteksi Serangan DDoS

Gambar 5 merupakan perbandingan F1-Score Antar Model untuk Deteksi Serangan DDoS, yang menampilkan diagram batang nilai F1-Score dari enam model deteksi anomali yang diuji — Deep SVDD, Isolation Forest, LOF, One-Class SVM, Autoencoder, dan Ensemble. F1-Score, sebagai rata-rata harmonik dari presisi dan recall, digunakan untuk menilai seberapa baik setiap model mencapai keseimbangan antara kemampuan mendeteksi serangan nyata dan meminimalkan alarm palsu, yang sangat krusial dalam skenario keamanan jaringan yang tidak seimbang. Dari visualisasi terlihat bahwa Deep SVDD mencatat F1-Score tertinggi (sekitar 0.886), menjadikannya model paling seimbang dan andal. LOF menempati posisi kedua dengan F1-Score sekitar 0.825, meskipun secara konsistensi performanya dipertanyakan karena AUC-nya rendah (0.500). Isolation Forest berada di posisi ketiga (~0.639), menunjukkan performa cukup baik namun jauh di bawah Deep SVDD. Sementara itu, One-Class SVM, Autoencoder, dan Ensemble memiliki F1-Score sangat rendah (sekitar 0.15–0.17), mengindikasikan kegagalan dalam mencapai keseimbangan deteksi yang bermakna. Secara keseluruhan, Gambar 3.3 memperkuat temuan bahwa Deep SVDD tidak hanya unggul dalam metrik diskriminasi (AUC), tetapi juga dalam keseimbangan praktis antara sensitivitas dan spesifisitas,

menjadikannya kandidat paling layak untuk implementasi sistem deteksi DDoS berbasis pembelajaran mesin.

3.4. Distribusi Skor Anomali: SVVD dan Baseline Model

Distribusi skor anomali dari keenam model — Deep SVDD, Isolation Forest, LOF, One-Class SVM, Autoencoder, dan Ensemble — disajikan dalam bentuk grafik histogram berganda dengan kurva KDE (Kernel Density Estimation), yang memperlihatkan bagaimana skor untuk kelas BENIGN (biru) dan DDoS (oranye) tersebar di ruang skor masing-masing model. Visualisasi ini memungkinkan analisis mendalam tentang sejauh mana setiap model mampu menciptakan pemisahan yang jelas antara lalu lintas normal dan serangan: semakin sedikit tumpang tindih antara dua distribusi, semakin baik kemampuan model dalam membedakan kelas tanpa bergantung pada threshold yang rumit. Sebaliknya, jika kedua distribusi saling menutupi atau memiliki puncak yang hampir identik, maka model tersebut cenderung menghasilkan banyak false positive atau false negative, terlepas dari parameter yang digunakan. Pemahaman atas pola distribusi ini sangat penting karena memberikan dasar intuitif mengapa suatu model mencatat AUC atau F1-Score tinggi atau rendah — bukan hanya angka, tapi juga *mengapa* angka itu muncul. Analisis ini akan membantu menjelaskan kekuatan dan kelemahan masing-masing pendekatan, serta memberikan wawasan tentang stabilitas dan interpretabilitas model dalam deteksi serangan DDoS nyata.



Gambar 6. Distribusi Skor Anomali untuk Keenam Model Deteksi Serangan DDoS

Gambar 6 menampilkan enam subplot yang masing-masing memvisualisasikan distribusi skor anomali dari satu model — Deep SVDD, Isolation Forest, LOF, One-Class SVM, Autoencoder, dan Ensemble — dengan membandingkan distribusi skor untuk kelas BENIGN (biru) dan DDoS (oranye) menggunakan histogram dan kurva KDE. Secara konsisten, Deep SVDD menunjukkan pemisahan paling jelas: sebagian besar sampel BENIGN terkonsentrasi di skor sangat rendah (hampir nol), sementara DDoS tersebar di skor lebih tinggi (hingga ~35), mencerminkan kemampuan encoder-nya belajar representasi laten yang efektif untuk membedakan anomali. Isolation Forest menunjukkan tumpang tindih signifikan antara kedua kelas, terutama di rentang skor 0.35–0.65, yang menjelaskan mengapa meskipun F1-Score-nya cukup baik, AUC-nya tidak setinggi Deep SVDD. LOF memiliki distribusi unik: hampir semua sampel BENIGN berada di skor sangat dekat nol, tetapi DDoS juga terkonsentrasi di skor rendah, menyebabkan tumpang tindih ekstrem — inilah alasan mengapa AUC-nya hanya 0.500. One-Class SVM dan Autoencoder menunjukkan pola serupa: sebagian besar BENIGN di skor rendah, namun DDoS hanya muncul di ujung kanan dengan jumlah sangat kecil, mengindikasikan bahwa model-model ini gagal menangkap karakteristik serangan secara luas. Ensemble, meskipun menggunakan rata-rata skor dari lima model, justru menghasilkan distribusi yang mirip Deep SVDD tapi lebih lebar dan lebih tumpang tindih, sehingga mengurangi ketajaman deteksi. Secara keseluruhan, Gambar 4.4 memberikan bukti visual kuat bahwa Deep SVDD adalah satu-satunya model yang berhasil menciptakan pemisahan kelas yang jelas dan stabil, yang menjadi dasar kuat bagi performa tinggi yang dicatatnya dalam metrik evaluasi sebelumnya.

3.5. Hasil Evaluasi Komparatif Model

Sebagai bagian inti dari evaluasi eksperimen, kinerja Deep SVDD yang diusulkan dibandingkan secara komprehensif terhadap lima model baseline deteksi anomali—Isolation Forest, Local Outlier Factor (LOF), One-Class SVM, Autoencoder, dan pendekatan Ensemble—menggunakan metrik evaluasi standar dalam deteksi intrusi jaringan. Tabel berikut menyajikan hasil kuantitatif dari keenam model berdasarkan AUC-ROC, Akurasi, Presisi, Recall, F1-Score, dan GFLOPs (hanya untuk Deep SVDD sebagai indikator efisiensi komputasi). Karena dataset bersifat tidak seimbang (jumlah BENIGN jauh lebih besar daripada DDoS), metrik seperti F1-Score dan Recall diberikan perhatian khusus, mengingat false negative dalam deteksi serangan memiliki konsekuensi keamanan yang sangat serius. Analisis berikut tidak hanya membandingkan angka, tetapi juga menghubungkan performa masing-masing model dengan karakteristik arsitektur, asumsi dasar, dan kemampuannya dalam menangkap pola serangan DDoS pada dataset UNSW-NB15.

Tabel 1 merangkum hasil evaluasi komprehensif dari enam model deteksi anomali pada dataset UNSW-NB15, menunjukkan bahwa Deep SVDD secara konsisten unggul dalam hampir semua metrik utama. Dengan AUC sebesar 0.805, Deep SVDD mencatat kemampuan diskriminasi terbaik antara lalu lintas normal dan serangan, diikuti oleh Isolation Forest (0.772) dan One-Class SVM (0.763). Lebih penting lagi, Deep SVDD mencapai recall tertinggi (90.99%), artinya hampir 91% serangan DDoS berhasil terdeteksi — sebuah keunggulan kritis dalam konteks keamanan siber. Presisinya yang tinggi (86.25%) menghasilkan F1-Score terbaik sebesar 0.886, jauh melampaui model lain. Isolation Forest menunjukkan presisi tinggi (81.87%) tetapi recall rendah (51.80%), sehingga F1-Score-nya hanya 0.635 — mengindikasikan bahwa ia terlalu konservatif dan melewatkan hampir separuh serangan. LOF menampilkan anomali menarik: meskipun F1-Score-nya 0.827 (kedua tertinggi), AUC-nya hanya 0.500, nyaris setara dengan

tebakan acak, yang menunjukkan bahwa performa F1-nya kemungkinan besar hasil dari threshold kebetulan, bukan kemampuan diskriminasi yang sebenarnya.

TABEL 1.
PERBANDINGAN KINERJA KUANTITATIF MODEL DETEKSI SERANGAN DDOS

Model	AUC	Accuracy	Precision	Recall	F1-Score	GFLOPs
Deep SVDD + Ensemble (Our)	**0.805301330 7**	**0.866620400 4**	**0.862466375 5**	**0.9099 146011**	**0.885555372 6**	**0.0004044 8**
Isolation Forest	0.772053129 9	0.661611836 3	0.818731739 4	0.5180 170798	0.634550064 6	N/A
LOF	0.500114953 9	0.812784241 9	0.869786426 7	0.7878 306603	0.826782518 4	N/A
One-Class SVM	0.763105853 7	0.423158703	0.457646755 9	0.0925 588419 1	0.153976091 5	N/A
Autoencoder	0.583802798 3	0.441881755 4	0.546980899 6	0.0924 546969 4	0.158173719 4	N/A

Sementara itu, One-Class SVM, Autoencoder, dan Ensemble semuanya memiliki recall sangat rendah (~9.2%), artinya mereka gagal mendeteksi lebih dari 90% serangan, sehingga meskipun akurasinya tinggi pada beberapa kasus, hal itu disebabkan oleh bias terhadap kelas mayoritas (BENIGN), bukan kemampuan deteksi nyata. Terakhir, Deep SVDD juga sangat efisien secara komputasi, dengan hanya 0.00040448 GFLOPs, menjadikannya kandidat ideal untuk deployment real-time. Secara keseluruhan, Tabel 4.1 membuktikan bahwa pendekatan berbasis representasi laten seperti Deep SVDD jauh lebih efektif dibanding metode tradisional dalam skenario deteksi DDoS yang realistis dan tidak seimbang.

3.6. Discusion

Temuan utama penelitian ini menegaskan bahwa Deep SVDD merupakan pendekatan paling efektif untuk deteksi serangan DDoS pada dataset UNSW-NB15, tidak hanya karena unggul dalam metrik utama (AUC = 0.805, F1-Score = 0.886, recall = 90.99%), tetapi juga karena kemampuannya menciptakan pemisahan kelas yang jelas dan stabil dalam distribusi skor anomali, serta konvergensi pelatihan yang andal. Keunggulan ini berasal dari arsitektur encoder berbasis representasi laten yang mampu menangkap pola kompleks lalu lintas normal, sehingga setiap penyimpangan signifikan (seperti lonjakan volume paket pada DDoS) secara otomatis menghasilkan skor tinggi. Sebaliknya, sebagian besar model baseline gagal mencapai keseimbangan deteksi yang bermakna: Isolation Forest terlalu konservatif (recall hanya 51.8%), One-Class SVM dan Autoencoder nyaris buta terhadap serangan (recall ~9.2%), dan yang mengejutkan, LOF menunjukkan F1-Score tinggi (0.827) namun AUC-nya 0.500 — sebuah kontradiksi yang mengungkap risiko menilai model hanya berdasarkan satu metrik tanpa melihat distribusi skor atau kurva ROC. Fenomena ini menunjukkan bahwa LOF mungkin "beruntung" menemukan threshold yang cocok untuk F1, tetapi tidak memiliki kemampuan diskriminasi intrinsik. Lebih mengejutkan lagi, pendekatan ensemble justru gagal meningkatkan performa, bahkan menurunkannya ke level Autoencoder, mengindikasikan bahwa rata-rata skor dari model heterogen tanpa pembobotan adaptif atau seleksi cerdas dapat melemahkan sinyal deteksi model terbaik. Temuan ini selaras dengan studi terkini yang menekankan bahwa ensemble dalam deteksi anomali hanya efektif jika komponennya berkualitas tinggi dan beragam secara bermakna (Wang et al., 2023). Selain itu, efisiensi komputasi Deep SVDD (0.0004 GFLOPs) membuka peluang untuk implementasi real-time pada sistem jaringan berkecepatan tinggi dengan sumber daya terbatas. Implikasi praktisnya jelas: dalam skenario keamanan siber, di mana false negative jauh lebih berbahaya daripada false positive, Deep SVDD menawarkan solusi yang tidak hanya akurat, tetapi juga andal, efisien, dan berdasarkan prinsip pembelajaran representasi yang kuat — menjadikannya kandidat utama untuk integrasi ke dalam sistem deteksi intrusi generasi berikutnya.

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa Deep SVDD, dengan arsitektur encoder berbasis representasi laten dan pelatihan berfokus pada data normal, mampu menghasilkan sistem deteksi serangan DDoS yang lebih andal, stabil, dan efisien dibandingkan pendekatan unsupervised konvensional. Model ini unggul karena kemampuannya mempelajari pola lalu lintas sah secara mendalam, sehingga penyimpangan akibat serangan dapat diidentifikasi dengan presisi tinggi tanpa bergantung pada label anomali. Sebaliknya, banyak metode baseline — termasuk ensemble sederhana — gagal mencapai keseimbangan deteksi yang bermakna, terutama karena keterbatasan dalam menangkap kompleksitas pola serangan modern.

Untuk penelitian lanjutan, arah yang menjanjikan meliputi: (1) pengembangan ensemble adaptif yang memberikan bobot dinamis berdasarkan kualitas skor tiap model; (2) integrasi Deep SVDD dengan mekanisme self-supervised learning untuk memperkaya representasi tanpa label; (3) evaluasi pada dataset multi-serangan dan skenario jaringan real-time; serta (4) optimasi arsitektur untuk deployment di perangkat edge dengan sumber daya terbatas. Dengan demikian, Deep SVDD bukan hanya solusi teknis, tetapi juga fondasi yang kuat untuk sistem keamanan siber adaptif di masa depan.

DAFTAR PUSTAKA

[1] I. H. Putro, "Evaluating the Performance of Machine Learning Classifiers for Network Intrusion Detection : A Comparative Study Using the," *TEKNIKA*, vol. 14, no. July, pp. 330–338, 2025, doi: 10.34148/teknika.v14i2.1276.

[2] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges," *Soft Comput.*, vol. 25, no. 15, pp. 9731–9763, Aug. 2021, doi: 10.1007/s00500-021-05893-0.

[3] A. Alharthi, M. Alaryani, and S. Kaddoura, "A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems," *Array*, vol. 26, no. April, p. 100406, 2025, doi: 10.1016/j.array.2025.100406.

[4] A. Syazweena and Z. Abdullah, "A Comparative Study between Machine Learning and Deep Learning Algorithm for Network Intrusion Detection," *J. SOFT Comput. DATA Min.*, vol. 2, pp. 43–51, 2022.

[5] P. Bountzis, D. Kavallieros, and T. Tsikrika, "A deep one-class classifier for network anomaly detection using autoencoders and one-class support vector machines," *Front. Comput. Sci.*, no. October, 2025, doi: 10.3389/fcomp.2025.1646679.

[6] T. Kenaza, K. Bennaceur, and A. Labed, "An efficient hybrid SVDD/clustering approach for anomaly-based intrusion detection," in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, in SAC '18. New York, NY, USA: Association for Computing Machinery, 2018, pp. 435–443. doi: 10.1145/3167132.3167180.

[7] W. Huang, Y. Li, Z. Xu, X. Yao, and R. Wan, "Improved Deep Support Vector Data Description Model Using Feature Patching for Industrial Anomaly Detection.," *Sensors (Basel).*, vol. 25, no. 1, Dec. 2024, doi: 10.3390/s25010067.

[8] M. Ahsan, H. Khusna, and M. H. Lee, "Support vector data description with kernel density estimation (SVDD - KDE) control chart for network intrusion monitoring," *Sci. Rep.*, pp. 1–12, 2023, doi: 10.1038/s41598-023-46719-3.

[9] Z. Zhang and X. Deng, "Anomaly detection using improved deep SVDD model with data structure preservation," *Pattern Recognit. Lett.*, vol. 148, pp. 1–6, 2021, doi: https://doi.org/10.1016/j.patrec.2021.04.020.

[10] B. H. Ali, N. Sulaiman, S. A. R. Al-Haddad, R. Atan, S. L. M. Hassan, and M. Alghrairi, "Identification of Distributed Denial of Services Anomalies by Ratio Test Methods," *Sensors*, pp. 1–17, 2021.

[11] F. Zhang, H. Fan, R. Wang, Z. Li, and T. Liang, "Deep Dual Support Vector Data description for anomaly detection on attributed networks," *Int. J. Intell. Syst.*, vol. 37, no. 2, pp. 1509–1528, 2022, doi: https://doi.org/10.1002/int.22683.

[12] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Comput. Secur.*, vol. 86, pp. 147–167, 2019, doi: https://doi.org/10.1016/j.cose.2019.06.005.

[13] M. Ieee, S. M. Ieee, M. Ieee, and M. Ieee, "A Unifying Review of Deep and Shallow Anomaly Detection," vol. 109, no. 5, 2021, doi: 10.1109/JPROC.2021.3052449.

[14] F. Pedregosa *et al.*, "Scikit-learn: Machine Learning in Python," *J. Mach. Learn. Res.*, vol. 12, no. null, pp. 2825–2830, Nov. 2011.

[15] Z. Alitbi, S. Amin, H. Seno, A. G. Bafghi, and D. Zabihzadeh, "A Generalized and Real-Time Network Intrusion Detection System Through Incremental Feature Encoding and Similarity Embedding Learning," *Sensors*, vol. 25, no. 16, pp. 1–24, 2025.

[16] W. Khan and M. Haroon, "An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks," *Int. J. Cogn. Comput. Eng.*, vol. 3, no. July, pp. 153–160, 2022, doi: 10.1016/j.ijcce.2022.08.002.

[17] Z. G. Ki, W. Somda, M. B. Kébré, and S. Gandema, "Machine Learning-Based Outlier Detection in Long-Term Climate Data : Evidence from Burkina Faso ' s Synoptic Network," *Atmos. Clim. Sci.*, vol. 15, no. 3, pp. 645–667, 2025, doi: 10.4236/acs.2025.153032.

[18] X. Liang, Y. Gao, and S. Xu, "ASE: Anomaly scoring based ensemble learning for highly imbalanced datasets," *Expert Syst. Appl.*, vol. 238, p. 122049, 2024, doi: https://doi.org/10.1016/j.eswa.2023.122049.

[19] G. Pang, C. Shen, L. Cao, and A. Van Den Hengel, "Deep Learning for Anomaly Detection: A Review," in *ACM Comput. Surv.*, New York, NY, USA: Association for Computing Machinery, Mar. 2021. doi: 10.1145/3439950.

[20] M. Shafi, A. H. Lashkari, and A. H. Roudsari, "Toward Generating a Large Scale Intrusion Detection Dataset and Intruders Behavioral Profiling Using Network and Transportation Layers Traffic Flow Analyzer (NTLFlowLyzer)," *J. Netw. Syst. Manag.*, vol. 33, no. 2, Mar. 2025, doi: 10.1007/s10922-025-09917-0.

[21] Y. Tian, J. Li, Q. Song, Z. Li, and X. Huang, "Pyramid reconstruction assisted deep autoencoding Gaussian mixture model for industrial fault detection," *Inf. Sci. (Ny).*, vol. 649, p. 119682, 2023, doi: https://doi.org/10.1016/j.ins.2023.119682.

[22] A. Duraj, N. Łukasik, and P. S. Szczepaniak, "Outlier Detection in EEG Signals Using Ensemble Classifiers," *Appl. Sci.*, vol. 15, no. 22, 2025, doi: 10.3390/app152212343.