

# Analisis Perbandingan CNN, SVM, dan Hybrid CNN-SVM untuk Deteksi Anomali Trafik Jaringan

Susiana Khosasih<sup>1,\*</sup>, Romi Antoni<sup>2</sup>, Ricky Irnanda<sup>3</sup>, Iswanto<sup>4</sup>, Rahmat Humala Putra Hasibuan<sup>5</sup>

<sup>1,2,3,4,5</sup> Fakultas Teknik Dan Ilmu Komputer, Program Studi Ilmu Komputer, Universitas Potensi Utama, Medan, Indonesia  
Email: <sup>1</sup>susianakhosasih21@gmail.com, <sup>2</sup>romi04antoni@gmail.com, <sup>3</sup>rickyirnanda17@gmail.com, <sup>4</sup>iswanto01982@gmail.com, <sup>5</sup>rahmathumala06@gmail.com

(\* Email Corresponding Author: susianakhosasih21@gmail.com)

Received: December 28, 2026 | Revision: January 6, 2026 | Accepted: January 6, 2026

## Abstrak

Peningkatan volume dan kompleksitas lalu lintas jaringan akibat pesatnya perkembangan teknologi informasi telah memicu munculnya ancaman keamanan siber yang semakin dinamis dan sulit diidentifikasi oleh sistem keamanan tradisional. Keterbatasan sistem deteksi berbasis *signature* dalam mengenali serangan baru, termasuk *zero-day attack*, menuntut penerapan pendekatan deteksi anomali yang lebih adaptif melalui pemanfaatan *machine learning* dan *deep learning* pada *Network Intrusion Detection System (NIDS)*. Penelitian ini bertujuan untuk menganalisis dan membandingkan kinerja model *Convolutional Neural Network (CNN)*, *Support Vector Machine (SVM)*, dan model *hybrid CNN-SVM* dalam mendeteksi anomali trafik jaringan. Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen untuk mengevaluasi performa ketiga model menggunakan dataset *CIC-IDS2017*. Eksperimen dilakukan melalui tahapan prapemrosesan data, pemodelan, serta evaluasi kinerja berdasarkan metrik *accuracy*, *precision*, *recall*, *F1-score*, dan *confusion matrix*. Hasil penelitian menunjukkan bahwa model *CNN* dan *SVM* sebagai *baseline* mampu mencapai tingkat akurasi yang tinggi, masing-masing sebesar 98,85% dan 98,66%, namun masih menunjukkan keterbatasan dalam mendeteksi kelas serangan minoritas. Model *hybrid CNN-SVM* memperoleh performa terbaik dengan akurasi 99,41% serta nilai *macro average recall* yang lebih seimbang, yang mengindikasikan peningkatan kemampuan generalisasi antar kelas. Integrasi *CNN* sebagai *feature extractor* dan *SVM* sebagai *classifier* terbukti efektif dalam memanfaatkan kompleksitas fitur trafik jaringan sekaligus meningkatkan stabilitas hasil klasifikasi. Dengan demikian, pendekatan *hybrid CNN-SVM* dapat direkomendasikan sebagai metode deteksi anomali trafik jaringan yang lebih efektif dan andal dibandingkan pendekatan tunggal dalam mendukung sistem keamanan jaringan modern.

**Kata Kunci:** *Network Intrusion Detection System, Anomaly Detection, Convolutional Neural Network, Support Vector Machine, Hybrid CNN-SVM*

## Abstract

The rapid growth of information technology has significantly increased the volume and complexity of network traffic, leading to cyber security threats that are increasingly dynamic and difficult to detect using traditional security systems. The limitations of signature-based detection systems in identifying new attacks, including zero-day attacks, necessitate the adoption of more adaptive anomaly detection approaches through the utilization of machine learning and deep learning within Network Intrusion Detection Systems (NIDS). This study aims to analyze and compare the performance of Convolutional Neural Networks (CNN), Support Vector Machines (SVM), and a hybrid CNN-SVM model in detecting network traffic anomalies. This research employs a quantitative approach using an experimental method to evaluate the performance of the three models based on the CIC-IDS2017 dataset. The experimental process includes data preprocessing, model development, and performance evaluation using accuracy, precision, recall, F1-score, and confusion matrix metrics. The results indicate that the CNN and SVM baseline models achieve high accuracy levels of 98.85% and 98.66%, respectively, but still exhibit limitations in detecting minority attack classes. The hybrid CNN-SVM model achieves the best performance with an accuracy of 99.41% and a more balanced macro-average recall, indicating improved generalization across classes. The integration of CNN as a feature extractor and SVM as a classifier is proven to be effective in leveraging the complexity of network traffic features while enhancing classification stability. Therefore, the hybrid CNN-SVM approach can be recommended as a more effective and reliable network traffic anomaly detection method compared to single-model approaches in supporting modern network security systems.

**Keywords:** *Network Intrusion Detection System, Anomaly Detection, Convolutional Neural Network, Support Vector Machine, Hybrid CNN-SVM*

## 1. PENDAHULUAN

Pertumbuhan pesat teknologi informasi dan komunikasi telah meningkatkan volume lalu lintas jaringan secara signifikan, sehingga ancaman keamanan siber menjadi semakin kompleks dan sulit diprediksi oleh sistem keamanan tradisional. Dalam beberapa dekade terakhir, karakter ancaman siber telah berkembang dari pola statis ke pola yang sangat dinamis, adaptif, dan tidak mudah diprediksi, termasuk serangan yang menggunakan teknik otomatisasi dan polimorfik untuk menghindari deteksi sistem keamanan konvensional [1]. Sifat ancaman siber yang semakin dinamis ini ditunjukkan oleh kemampuan para penyerang untuk menciptakan pola serangan yang berubah-ubah dan sulit dikenali oleh sistem berbasis tanda tangan (*signature-based*) [2].

Serangan jaringan modern seperti zero-day attack memanfaatkan celah keamanan yang sama sekali belum diketahui atau diperbaiki, sehingga pihak pengembang maupun sistem keamanan tidak memiliki pertahanan awal yang memadai, dan hal ini menunjukkan keterbatasan sistem berbasis signature dalam mendeteksi ancaman yang belum terdokumentasi. Zero-day attack merupakan salah satu bentuk ancaman siber yang sulit dideteksi oleh sistem keamanan tradisional karena tidak ada patch atau tanda tangan serangan yang tersedia saat eksploitasi pertama kali terjadi, yang menyebabkan penyerang dapat beroperasi tanpa terdeteksi dalam waktu yang lama. Karena sifatnya yang tersembunyi dan prediktabilitasnya yang rendah, serangan zero-day memperlihatkan bahwa sistem keamanan berbasis signature, seperti intrusion detection system konvensional, sering kali gagal dalam mengidentifikasi aktivitas berbahaya yang belum pernah terjadi sebelumnya [3][4]. Sistem signature-based intrusion detection hanya mampu mengenali serangan yang telah terdefinisi sebelumnya karena metode ini mengandalkan kecocokan pola serangan yang sudah ada dalam basis data tanda tangan, sehingga tidak dapat mendeteksi ancaman baru yang belum terekam, ketergantungan pada basis data serangan membuat sistem konvensional kurang adaptif terhadap pola serangan baru karena setiap jenis serangan baru harus terlebih dahulu didefinisikan dalam basis data tanda tangan sebelum dapat dikenali oleh sistem. Kondisi ini menuntut pendekatan deteksi yang lebih fleksibel dan adaptif terhadap perubahan pola trafik jaringan [5]. Network Intrusion Detection System (NIDS) berperan penting dalam menjaga keamanan jaringan dengan memantau dan menganalisis lalu lintas data, pendekatan anomaly-based NIDS dinilai lebih efektif dalam mendeteksi penyimpangan perilaku trafik jaringan karena tidak hanya mendeteksi serangan yang sudah dikenal tetapi juga dapat mengenali perilaku abnormal yang tidak pernah terlihat sebelumnya. Metode berbasis anomali memungkinkan identifikasi aktivitas mencurigakan tanpa ketergantungan pada signature serangan, dengan cara membangun model perilaku normal terlebih dahulu sehingga setiap penyimpangan yang signifikan dari model tersebut dapat dianggap sebagai potensi ancaman [6]. Peningkatan skala dan heterogenitas data trafik jaringan mendorong pemanfaatan metode machine learning dan deep learning dalam deteksi anomali, karena kedua pendekatan ini mampu belajar dari data besar secara otomatis untuk membedakan antara perilaku normal dan abnormal. Machine learning dan deep learning menjadi fondasi utama dalam pengembangan sistem deteksi intrusi modern, terutama ketika sistem perlu beradaptasi terhadap variasi ancaman yang tidak dapat diprediksi melalui metode tradisional [5].

Convolutional Neural Network (CNN) merupakan algoritma *deep learning* yang banyak digunakan dalam sistem deteksi intrusi jaringan karena kemampuannya dalam mempelajari pola kompleks dari data trafik secara otomatis. CNN efektif dalam membedakan trafik normal dan anomali melalui proses ekstraksi fitur hierarkis menggunakan lapisan konvolusi, sehingga mengurangi ketergantungan pada proses *feature engineering* manual. Keunggulan CNN terletak pada kemampuannya menangkap hubungan spasial dan pola nonlinier yang kompleks, yang membuatnya sering menghasilkan performa klasifikasi yang lebih adaptif dan akurat, khususnya pada dataset jaringan berskala besar dan berdimensi tinggi [7]. SVM merupakan algoritma machine learning yang banyak digunakan dalam sistem deteksi intrusi karena kemampuannya menangani masalah klasifikasi berdimensi tinggi. SVM sering digunakan untuk klasifikasi biner antara trafik normal dan anomali dengan performa yang stabil, terutama pada dataset benchmark yang telah diproses dengan feature extraction standar. Keunggulan SVM terletak pada kemampuannya membangun batas keputusan optimal yang kuat, sehingga SVM sering kali memberikan hasil klasifikasi yang stabil dan akurat dalam banyak kasus deteksi anomali jaringan [8]. Pendekatan hybrid CNN-SVM mengombinasikan CNN sebagai feature extractor dan SVM sebagai pengklasifikasi sehingga memanfaatkan kekuatan masing-masing metode untuk deteksi anomali jaringan. Model hybrid bertujuan memanfaatkan keunggulan CNN dalam ekstraksi fitur dan kekuatan SVM dalam klasifikasi sehingga dapat meningkatkan akurasi deteksi sekaligus mempertahankan stabilitas hasil [9].

Meskipun banyak studi telah menerapkan berbagai teknik machine learning dan deep learning untuk intrusion detection, termasuk model hybrid, masih terdapat kekurangan dalam melakukan perbandingan langsung yang komprehensif antara CNN, SVM, dan model hybrid CNN-SVM dalam satu kerangka eksperimen yang konsisten serta evaluasi terhadap berbagai kondisi dataset dan metrik performa, yang menunjukkan kebutuhan penelitian yang lebih terstandar dan menyeluruh di area ini [10]. Oleh karena itu, penelitian ini bertujuan menganalisis dan membandingkan kinerja model CNN, SVM, dan hybrid CNN-SVM dalam deteksi anomali trafik jaringan, sehingga dapat mengetahui metode mana yang paling efektif dalam berbagai scenario dan memberikan rekomendasi pemilihan model deteksi anomali yang paling efektif dan efisien untuk sistem keamanan jaringan modern, berdasarkan hasil evaluasi komparatif tersebut.

## 2. METODOLOGI PENELITIAN

Metodologi penelitian merupakan landasan penting dalam menjalankan suatu penelitian ilmiah. Bab ini menjelaskan secara sistematis pendekatan, metode, dan prosedur yang digunakan untuk menganalisis performa model deteksi anomali trafik jaringan menggunakan CNN, SVM, dan hybrid CNN-SVM. Penelitian ini bertujuan untuk membandingkan efektivitas ketiga metode dalam mendeteksi anomali jaringan, sehingga diperlukan rancangan penelitian yang terstruktur mulai dari pengumpulan data, praproses, pelatihan model, hingga evaluasi kinerja. Dengan

metodologi yang jelas dan sistematis, hasil penelitian diharapkan dapat memberikan pemahaman yang akurat mengenai keunggulan dan kelemahan masing-masing metode, sekaligus memberikan dasar yang kuat bagi penelitian selanjutnya di bidang deteksi anomali trafik jaringan.

## 2.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan penelitian kuantitatif, yaitu pendekatan yang menitikberatkan pada pengumpulan dan analisis data numerik serta pengujian hipotesis secara sistematis. Dalam metodologi kuantitatif, salah satu desain penelitian utama adalah desain eksperimen, yang digunakan untuk menguji hubungan sebab-akibat antar variabel melalui manipulasi dan kontrol variabel yang relevan [11]. Metode yang diterapkan dalam penelitian ini adalah metode eksperimen, yang memungkinkan pengujian terkontrol terhadap beberapa model klasifikasi untuk menganalisis dan membandingkan kinerjanya, khususnya Convolutional Neural Network (CNN), Support Vector Machine (SVM), dan model hybrid CNN-SVM, dalam mendeteksi anomali trafik jaringan [12].

## 2.2 Metode Pengumpulan Data

Dataset yang digunakan dalam penelitian ini adalah CIC-IDS2017, yaitu dataset deteksi intrusi yang dikembangkan oleh Canadian Institute for Cybersecurity (CIC). Dataset ini dirancang untuk menggambarkan kondisi trafik jaringan yang realistis dengan mencakup trafik normal (benign) serta berbagai jenis serangan siber modern, seperti *Denial of Service (DoS)*, *Distributed Denial of Service (DDoS)*, *Brute Force*, *Web Attack*, dan serangan jaringan lainnya. CIC-IDS2017 menyediakan fitur-fitur numerik hasil ekstraksi aliran jaringan (*network flow*) yang komprehensif dan telah dilabeli, sehingga banyak digunakan sebagai dataset benchmark dalam penelitian *Intrusion Detection System* berbasis *machine learning* dan *deep learning*. Karakteristik tersebut menjadikan CIC-IDS2017 sesuai digunakan sebagai data masukan dalam proses pelatihan dan pengujian model deteksi intrusi jaringan [13].

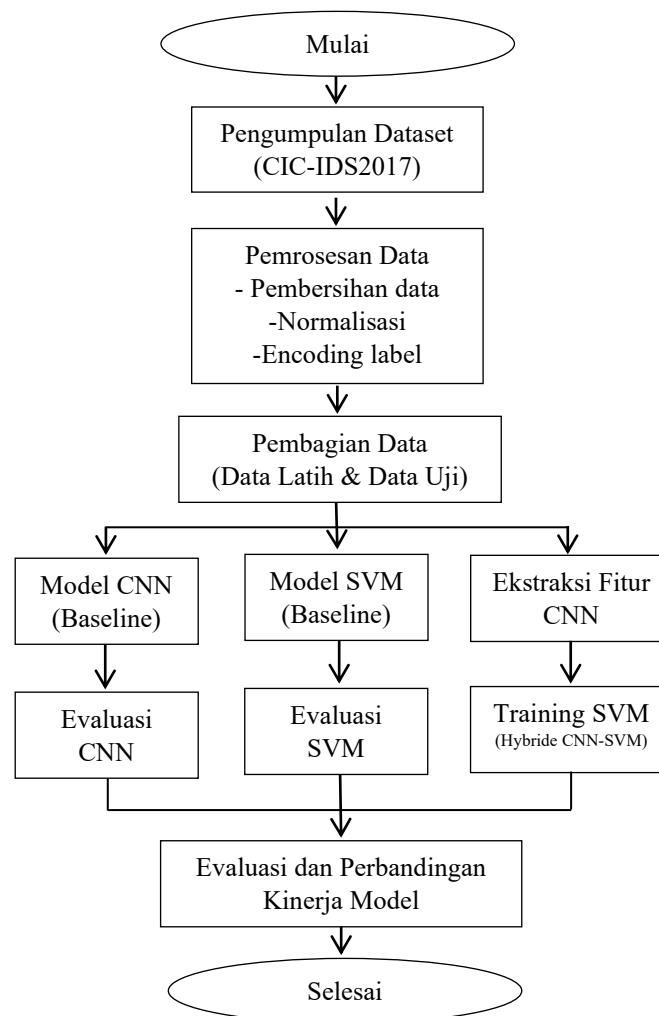
### 2.2.1 Justifikasi Pemilihan Dataset CIC-IDS2017

Dataset CIC-IDS2017 dipilih karena merupakan dataset benchmark yang secara luas digunakan dalam penelitian Network Intrusion Detection System (NIDS) berbasis machine learning dan deep learning. Dataset ini merepresentasikan trafik jaringan yang realistis melalui kombinasi trafik normal (benign) dan berbagai jenis serangan modern, sehingga relevan untuk evaluasi sistem deteksi anomali. CIC-IDS2017 menggunakan pendekatan flow-based features dengan fitur numerik berdimensi tinggi yang mencerminkan karakteristik statistik trafik jaringan. Karakteristik ini sesuai untuk mengevaluasi kemampuan CNN dalam mengekstraksi pola nonlinier serta SVM dalam membangun batas keputusan yang optimal pada ruang fitur berdimensi tinggi.

Namun demikian, dataset ini memiliki distribusi kelas yang tidak seimbang, di mana trafik normal mendominasi sebagian besar data. Kondisi ini berpotensi menghasilkan nilai akurasi yang sangat tinggi. Oleh karena itu, dalam penelitian ini akurasi tidak dijadikan satu-satunya indikator performa, melainkan dianalisis bersama macro-average recall dan F1-score untuk menilai kemampuan model dalam mendeteksi kelas serangan minoritas. Dengan pendekatan evaluasi tersebut, performa model dapat dianalisis secara lebih objektif dan tidak bias terhadap karakteristik dataset.

## 2.3 Tahapan Penelitian

Penelitian ini dilaksanakan melalui serangkaian tahapan yang tersusun secara sistematis untuk memastikan proses analisis dan evaluasi model berjalan secara terstruktur dan terkontrol. Dalam penelitian berbasis metode eksperimen, tahapan penelitian dirancang secara berurutan guna menjamin objektivitas dan konsistensi hasil evaluasi. Setiap tahapan penelitian disusun untuk mendukung tujuan utama penelitian, yaitu menganalisis dan membandingkan kinerja model CNN, SVM, dan hybrid CNN-SVM dalam mendeteksi anomali trafik jaringan menggunakan dataset CIC-IDS2017 [14]. Alur tahapan penelitian ditunjukkan pada Gambar 1.



**Gambar 1.** Tahapan Penelitian

Penelitian diawali dengan pengumpulan *dataset* CIC-IDS2017 yang memuat trafik jaringan normal dan berbagai jenis serangan. Dataset tersebut kemudian melalui tahap prapemrosesan yang mencakup pembersihan data, normalisasi fitur numerik, serta pengkodean label kelas. Setelah itu, data dibagi menjadi data latih dan data uji untuk memastikan evaluasi model dilakukan secara objektif. Pada tahap pemodelan, CNN dan SVM dibangun sebagai model *baseline*. CNN digunakan untuk melakukan klasifikasi langsung terhadap data trafik jaringan, sedangkan SVM dilatih menggunakan fitur numerik hasil prapemrosesan. Selanjutnya, model *hybrid* CNN–SVM dikembangkan dengan memanfaatkan CNN sebagai *feature extractor* dan SVM sebagai *classifier*. Tahap akhir penelitian adalah evaluasi dan perbandingan kinerja seluruh model menggunakan metrik akurasi, presisi, *recall*, *f1-score*, serta *confusion matrix*. Hasil evaluasi tersebut digunakan untuk menganalisis keunggulan dan keterbatasan masing-masing model sebagai dasar dalam penarikan kesimpulan.

### 2.3.1 Mekanisme Model Hybrid CNN–SVM

Model hybrid CNN–SVM dirancang untuk memanfaatkan keunggulan komplementer dari CNN dan SVM. CNN digunakan secara eksklusif sebagai *feature extractor*, bukan sebagai pengklasifikasi akhir. Melalui lapisan konvolusi, CNN mempelajari representasi fitur laten yang lebih diskriminatif dari data trafik jaringan dibandingkan fitur numerik mentah. Fitur hasil ekstraksi CNN kemudian digunakan sebagai masukan bagi SVM, yang berperan sebagai *classifier*. Pemilihan SVM didasarkan pada kemampuannya dalam melakukan *margin maximization*, sehingga menghasilkan batas keputusan yang lebih stabil dan robust pada fitur berdimensi tinggi. Pendekatan hybrid ini tidak didasarkan pada asumsi kelemahan CNN atau SVM secara individual, melainkan pada strategi integrasi. CNN unggul dalam menangkap kompleksitas pola trafik jaringan, sementara SVM meningkatkan stabilitas dan kemampuan generalisasi pada tahap klasifikasi. Dengan demikian, model hybrid CNN–SVM diharapkan mampu memberikan performa yang lebih seimbang dibandingkan pendekatan tunggal.

## 2.4 Spesifikasi Perangkat Penelitian

Penelitian ini dilaksanakan menggunakan kombinasi perangkat keras dan perangkat lunak yang mendukung proses pengolahan data berskala besar serta pelatihan model *machine learning* dan *deep learning*. Seluruh proses pemrograman dan eksperimen dilakukan menggunakan platform cloud computing Google Colaboratory, yang menyediakan lingkungan pemrograman berbasis *Jupyter Notebook* dengan akses GPU/TPU yang memadai untuk pelatihan model tanpa ketergantungan pada spesifikasi perangkat lokal [15]. Adapun spesifikasi lingkungan penelitian yang digunakan disajikan pada Tabel 1.

**Tabel 1.** Spesifikasi Perangkat

Komponen	Spesifikasi
Prosesor	AMD Ryzen 5 5600H with Radeon Graphics (3.30 GHz)
Memori	8,00 GB
Sistem Operasi	Windows 11 64-bit
Platform Pemrograman	Google Colaboratory
Bahasa Pemrograman	Python
Library Utama	TensorFlow, Keras, Scikit-learn, NumPy, Pandas, Matplotlib
Lingkungan Eksekusi	Cloud-based environment (Google Colab)

## 2.5 Rumus Evaluasi Kinerja Model

Evaluasi kinerja model klasifikasi pada penelitian ini dilakukan menggunakan *confusion matrix* yang terdiri dari empat komponen utama, yaitu *True Positive* (TP), *True Negative* (TN), *False Positive* (FP), dan *False Negative* (FN). Berdasarkan komponen tersebut, metrik evaluasi yang digunakan didefinisikan sebagai berikut.

### 1. Akurasi (*Accuracy*)

Akurasi menunjukkan tingkat ketepatan model dalam mengklasifikasikan seluruh data uji secara benar.

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

### 2. Presisi (*Precision*)

Presisi mengukur kemampuan model dalam mengklasifikasikan data positif secara tepat.

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

### 3. Recall (*Sensitivity*)

*Recall* menunjukkan kemampuan model dalam mendeteksi seluruh data positif yang sebenarnya.

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

### 4. F1-Score

*F1-score* merupakan rata-rata harmonik antara *precision* dan *recall*, yang digunakan untuk menyeimbangkan kedua metrik tersebut.

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

### 5. Confusion Matrix

*Confusion matrix* digunakan untuk memberikan gambaran detail terkait hasil klasifikasi model pada setiap kelas, sehingga memudahkan analisis kesalahan prediksi dan performa model secara menyeluruh.

## 3.HASIL DAN PEMBAHASAN

Eksperimen deteksi anomali trafik jaringan dilakukan menggunakan tiga pendekatan klasifikasi, yaitu CNN, SVM, dan hybrid CNN-SVM, dengan memanfaatkan dataset CIC-IDS2017. CNN dan SVM difungsikan sebagai baseline guna

memberikan acuan kinerja terhadap model hybrid. Evaluasi dilakukan berdasarkan metrik akurasi dan kualitas klasifikasi untuk menilai kemampuan setiap model dalam membedakan trafik normal dan anomali.

### 3.1 Deskripsi Dataset CIC-IDS2017 dan Karakteristik Data

Berdasarkan hasil pemuatan data, dataset CIC-IDS2017 yang digunakan dalam penelitian ini terdiri dari 543.734 instance dengan 79 atribut, di mana satu atribut berperan sebagai label kelas dan sisanya merupakan fitur numerik yang merepresentasikan karakteristik aliran trafik jaringan (*flow-based features*). Fitur-fitur tersebut mencakup informasi terkait durasi aliran, jumlah paket, panjang paket, statistik waktu aktif (*active time*) dan waktu idle (*idle time*), serta karakteristik forward dan backward packet.

Label pada dataset menunjukkan dua kategori utama, yaitu trafik normal (BENIGN) dan trafik anomali, yang mencakup berbagai jenis serangan seperti *DoS*, *PortScan*, *Brute Force*, dan serangan lainnya. Keberagaman jenis serangan ini menjadikan CIC-IDS2017 sebagai dataset yang menantang dan representatif untuk mengevaluasi performa sistem deteksi anomali jaringan.

Seluruh fitur pada dataset berbentuk numerik sehingga dapat langsung digunakan pada proses pelatihan model setelah melalui tahap prapemrosesan. Dimensi fitur yang relatif tinggi mencerminkan kompleksitas pola trafik jaringan, sehingga pendekatan pembelajaran mesin dan pembelajaran mendalam diperlukan untuk mengekstraksi informasi yang relevan secara efektif. Dataset ini digunakan secara konsisten pada seluruh skenario pengujian, baik untuk model CNN, SVM, maupun model hybrid CNN-SVM, guna memastikan perbandingan kinerja dilakukan secara adil (*fair comparison*).

### 3.2 Hasil Pengujian Model Baseline CNN

Model Convolutional Neural Network (CNN) digunakan sebagai baseline dalam mendeteksi anomali trafik jaringan pada dataset CIC-IDS2017. Evaluasi dilakukan menggunakan metrik accuracy, precision, recall, dan F1-score pada data uji yang sama dengan model lainnya.

**Tabel 2.** Hasil Pengujian CNN

Metrik	Nilai
Accuracy	0,9885
Precision (Weighted Avg)	0,99
Recall (Weighted Avg)	0,99
F1-score (Weighted Avg)	0,99
Macro Avg Recall	0,75
Macro Avg F1-score	0,77
Jumlah Data Uji	108.614

Hasil pengujian menunjukkan bahwa CNN mencapai akurasi 98,85%, yang menandakan kemampuan klasifikasi yang sangat baik secara keseluruhan. Nilai metrik berbobot yang tinggi menunjukkan performa optimal pada kelas mayoritas. Namun, nilai macro average recall yang lebih rendah mengindikasikan keterbatasan CNN dalam mendeteksi kelas serangan minoritas. Kondisi ini menunjukkan adanya bias terhadap distribusi data yang tidak seimbang pada CIC-IDS2017. Oleh karena itu, CNN sebagai baseline memiliki akurasi global yang tinggi, tetapi masih memerlukan pendekatan tambahan untuk meningkatkan deteksi pada kelas serangan yang jarang muncul, yang menjadi dasar penggunaan model hybrid CNN-SVM.

### 3.2 Hasil Pengujian Model Baseline SVM

Model Support Vector Machine (SVM) digunakan sebagai baseline pembanding terhadap CNN dan model hybrid CNN-SVM dalam mendeteksi anomali trafik jaringan pada dataset CIC-IDS2017. Evaluasi kinerja dilakukan menggunakan metrik accuracy, precision, recall, dan F1-score pada data uji yang sama.

**Tabel 3.** Hasil Pengujian SVM

Metrik	Nilai
Accuracy	0,9866
Precision (Weighted Avg)	0,99
Recall (Weighted Avg)	0,99
F1-score (Weighted Avg)	0,99
Macro Avg Recall	0,81
Macro Avg F1-score	0,80

Jumlah Data Uji 108.614

Hasil pengujian menunjukkan bahwa model SVM mencapai akurasi sebesar 98,66%, sedikit lebih rendah dibandingkan model CNN. Metrik berbobot yang tinggi menunjukkan bahwa SVM mampu mengklasifikasikan kelas mayoritas dengan baik. Jika dibandingkan dengan CNN, model SVM menunjukkan nilai macro average recall yang lebih tinggi, yang mengindikasikan kemampuan yang lebih baik dalam mendeteksi kelas serangan minoritas. Namun demikian, performa SVM masih terbatas pada beberapa kelas dengan jumlah data sangat kecil, yang ditunjukkan oleh rendahnya nilai precision dan recall pada kelas tertentu. Secara keseluruhan, SVM sebagai baseline memiliki kemampuan generalisasi yang lebih seimbang dibandingkan CNN, tetapi masih belum optimal dalam memanfaatkan kompleksitas fitur trafik jaringan berdimensi tinggi. Keterbatasan ini menjadi dasar perlunya pendekatan hybrid untuk menggabungkan keunggulan CNN dan SVM.

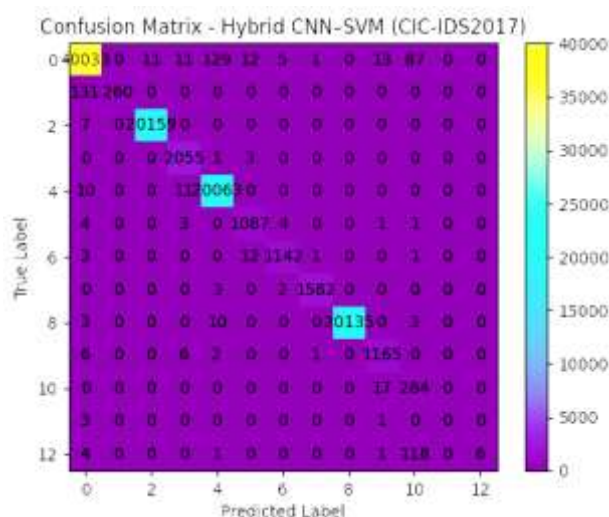
### 3.3 Hasil Pengujian Model Hybrid CNN - SVM

Model hybrid CNN–SVM dikembangkan dengan menggabungkan kemampuan CNN sebagai ekstraktor fitur dan SVM sebagai pengklasifikasi. Pada tahap ini, CNN menghasilkan representasi fitur berdimensi 128 dari 78 fitur input, yang selanjutnya digunakan sebagai masukan untuk proses pelatihan dan pengujian SVM. Pendekatan ini bertujuan untuk meningkatkan kemampuan klasifikasi dengan memanfaatkan fitur yang lebih diskriminatif. Hasil ekstraksi fitur menunjukkan bahwa data latih dan data uji masing-masing menghasilkan vektor fitur berukuran (434.453, 128) dan (108.614, 128), yang menandakan proses ekstraksi fitur berjalan dengan baik dan konsisten.

**Tabel 4.** Hasil Pengujian *Hybrid* CNN-SVM

Metrik	Nilai
Accuracy	0,9941
Precision (Weighted Avg)	0,99
Recall (Weighted Avg)	0,99
F1-score (Weighted Avg)	0,99
Macro Avg Recall	0,82
Macro Avg F1-score	0,81
Jumlah Data Uji	108.614

Model hybrid CNN–SVM mencapai akurasi sebesar 99,41%, yang merupakan nilai tertinggi dibandingkan model CNN dan SVM sebagai baseline. Peningkatan ini menunjukkan bahwa fitur yang dihasilkan oleh CNN mampu meningkatkan kinerja SVM dalam membedakan trafik normal dan anomali. Jika ditinjau dari macro average recall, model hybrid menunjukkan nilai yang lebih baik dibandingkan CNN dan sebanding dengan SVM, yang mengindikasikan peningkatan kemampuan dalam mendeteksi kelas serangan minoritas. Hal ini menunjukkan bahwa integrasi CNN dan SVM mampu mengurangi kelemahan masing-masing model ketika digunakan secara terpisah. Secara keseluruhan, hasil ini membuktikan bahwa pendekatan hybrid CNN–SVM memberikan keseimbangan antara akurasi global dan kemampuan generalisasi antar kelas, sehingga lebih efektif digunakan untuk deteksi anomali trafik jaringan pada dataset CIC-IDS2017.



**Gambar 2.** Confusion Matrix Hybrid CNN-SVM

Confusion matrix pada Gambar 2 menunjukkan bahwa sebagian besar hasil klasifikasi model hybrid CNN–SVM terkonsentrasi pada diagonal utama, yang mengindikasikan tingkat prediksi yang tinggi dan konsisten pada berbagai kelas trafik jaringan. Model menunjukkan performa yang sangat baik pada kelas dengan jumlah data besar, dengan tingkat kesalahan klasifikasi yang relatif rendah. Meskipun masih terdapat mis-klasifikasi pada beberapa kelas minoritas akibat ketidakseimbangan distribusi data pada dataset CIC-IDS2017, hal tersebut tidak berdampak signifikan terhadap kinerja keseluruhan model. Secara umum, hasil ini menegaskan bahwa pendekatan hybrid CNN–SVM mampu memberikan keseimbangan yang lebih baik antara akurasi global dan kemampuan generalisasi dibandingkan model baseline.

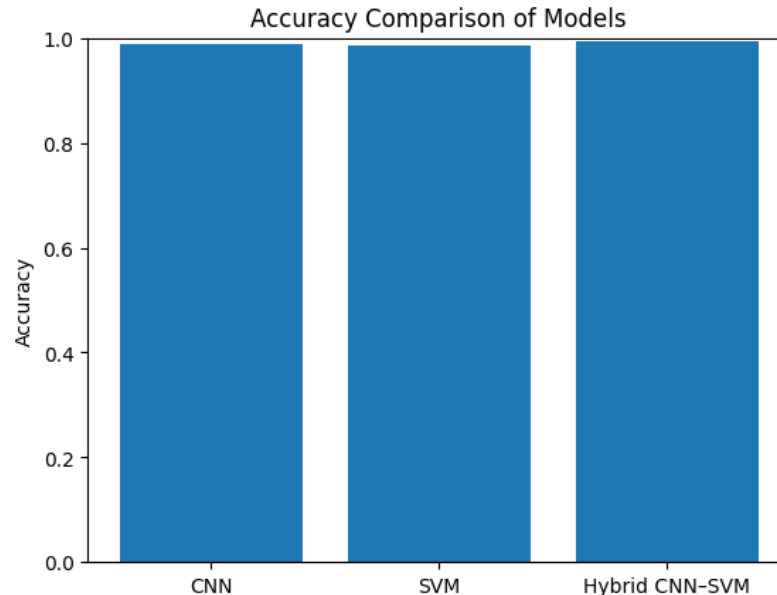
### 3.4 Analisis Perbandingan Kinerja Model

Perbandingan kinerja dilakukan untuk mengevaluasi efektivitas model CNN, SVM, dan hybrid CNN–SVM dalam mendeteksi anomali trafik jaringan pada dataset CIC-IDS2017. Seluruh model diuji menggunakan skenario pengujian yang sama sehingga hasil yang diperoleh dapat dibandingkan secara objektif.

**Tabel 5.** Analisis Perbandingan Kinerja Model

Model	Accuracy
CNN	0,9885
SVM	0,9866
Hybrid CNN–SVM	0,9941

Berdasarkan Tabel 3.5, model hybrid CNN–SVM memperoleh nilai akurasi tertinggi, yaitu 99,41%, dibandingkan dengan model CNN dan SVM sebagai baseline. Hasil ini menunjukkan bahwa integrasi CNN sebagai ekstraktor fitur dan SVM sebagai pengklasifikasi mampu meningkatkan kinerja deteksi anomali secara keseluruhan. Model CNN menunjukkan performa yang sangat baik, namun masih sedikit lebih rendah dibandingkan model hybrid, sedangkan SVM memperoleh akurasi terendah di antara ketiga model.



**Gambar 3.** Diagram *Accuracy Comparison*

Gambar 3 memperlihatkan perbandingan visual akurasi ketiga model, di mana model hybrid CNN–SVM menunjukkan peningkatan yang paling signifikan. Visualisasi ini mempertegas bahwa pendekatan hybrid memberikan performa yang lebih stabil dibandingkan pendekatan tunggal. Peningkatan akurasi ini menunjukkan bahwa fitur hasil ekstraksi CNN lebih efektif ketika dikombinasikan dengan kemampuan SVM dalam memisahkan kelas, sehingga menghasilkan sistem deteksi anomali yang lebih andal pada dataset CIC-IDS2017.

### 3.5 Analisis Potensi Overfitting dan Generalisasi Model

Perolehan nilai akurasi yang sangat tinggi menimbulkan potensi overfitting, khususnya mengingat penggunaan dataset benchmark dengan distribusi kelas yang tidak seimbang. Untuk mengurangi bias tersebut, evaluasi model dilakukan pada data uji terpisah serta tidak hanya mengandalkan akurasi, tetapi juga mempertimbangkan macro-average

recall dan F1-score. Hasil evaluasi menunjukkan bahwa meskipun akurasi global tinggi, nilai macro-average recall relatif lebih rendah, yang mengindikasikan bahwa tantangan utama masih terletak pada deteksi kelas minoritas. Model hybrid CNN-SVM menunjukkan keseimbangan performa yang lebih baik dibandingkan model baseline, namun belum sepenuhnya menghilangkan pengaruh karakteristik dataset. Selain itu, penggunaan CIC-IDS2017 yang bersifat offline dan single-domain membatasi generalisasi model terhadap trafik jaringan real-time. Oleh karena itu, hasil penelitian ini belum dapat diklaim sepenuhnya bebas dari overfitting terhadap dataset tertentu. Temuan ini menunjukkan bahwa performa tinggi yang diperoleh perlu divalidasi lebih lanjut melalui pengujian lintas dataset dan skenario real-time untuk memastikan kemampuan generalisasi model secara menyeluruh.

### 3.6 Ringkasan Pembahasan Hasil

Berdasarkan hasil pengujian dan analisis perbandingan, ketiga model yang diuji, yaitu CNN, SVM, dan hybrid CNN-SVM, mampu mendeteksi anomali trafik jaringan pada dataset CIC-IDS2017 dengan tingkat akurasi yang tinggi. Model CNN menunjukkan kemampuan yang sangat baik dalam mempelajari pola trafik dominan, sementara SVM memberikan performa yang relatif lebih seimbang dalam mendeteksi beberapa kelas minoritas. Namun demikian, model hybrid CNN-SVM secara konsisten menghasilkan performa terbaik dengan keseimbangan yang lebih baik antara akurasi global dan kemampuan generalisasi antar kelas. Integrasi CNN sebagai ekstraktor fitur dan SVM sebagai pengklasifikasi terbukti efektif dalam menangani kompleksitas fitur berdimensi tinggi serta mengurangi bias terhadap kelas mayoritas. Meskipun demikian, performa tinggi yang diperoleh masih dipengaruhi oleh karakteristik dataset CIC-IDS2017, sehingga validasi lanjutan pada skenario dan dataset yang berbeda tetap diperlukan.

## 4. KESIMPULAN

Penelitian ini berhasil melakukan analisis perbandingan kinerja model *Convolutional Neural Network* (CNN), *Support Vector Machine* (SVM), dan model *hybrid* CNN-SVM dalam mendeteksi anomali trafik jaringan menggunakan dataset CIC-IDS2017. CNN dan SVM digunakan sebagai model *baseline* untuk mengevaluasi efektivitas pendekatan hibrida yang mengintegrasikan kemampuan CNN dalam mengekstraksi fitur secara otomatis dan SVM dalam melakukan klasifikasi. Pendekatan ini dirancang untuk memanfaatkan keunggulan masing-masing metode dalam menangani data trafik jaringan berdimensi tinggi dan kompleks. Hasil eksperimen menunjukkan bahwa ketiga model mampu mencapai tingkat akurasi yang tinggi. Namun demikian, model *hybrid* CNN-SVM secara konsisten memberikan performa terbaik dengan akurasi sebesar 99,41%, serta menunjukkan keseimbangan yang lebih baik antara akurasi global dan kemampuan generalisasi antar kelas dibandingkan pendekatan tunggal. Integrasi CNN sebagai *feature extractor* dan SVM sebagai *classifier* terbukti mampu meningkatkan stabilitas batas keputusan dan mengurangi bias terhadap kelas mayoritas. Analisis *confusion matrix* dan metrik evaluasi juga mengonfirmasi bahwa pendekatan hibrida mampu menurunkan tingkat kesalahan klasifikasi pada beberapa kelas serangan dibandingkan model CNN dan SVM secara terpisah, meskipun deteksi terhadap kelas minoritas dengan jumlah data yang sangat terbatas masih menjadi tantangan. Keterbatasan utama penelitian ini terletak pada penggunaan dataset CIC-IDS2017 yang bersifat *offline* dan memiliki distribusi kelas yang tidak seimbang, sehingga performa model belum sepenuhnya merepresentasikan kondisi trafik jaringan secara *real-time*. Selain itu, penelitian ini belum mengevaluasi aspek efisiensi komputasi dan latensi inferensi yang penting dalam implementasi sistem deteksi intrusi di lingkungan nyata. Oleh karena itu, penelitian selanjutnya disarankan untuk melakukan pengujian lintas dataset dan skenario *real-time*, menerapkan teknik penanganan ketidakseimbangan data, serta mengintegrasikan pendekatan *explainable artificial intelligence* (XAI) guna meningkatkan interpretabilitas dan keandalan sistem deteksi anomali jaringan.

## REFERENCES

- [1] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, "MANAJEMEN KEAMANAN CYBER DI ERA DIGITAL," *Journal of Business And Entrepreneurship*, vol. 11, no. 1, p. 23, Jun. 2023, doi: 10.46273/job.e.v11i1.365.
- [2] Ade Irawan, Wildan Hamzah Nur Fadholi, Zahwa Erikamaretha, and Fried Sinlae, "Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT," *JOURNAL ZETROEM*, vol. 6, no. 1, pp. 114–119, Apr. 2024, doi: 10.36526/ztr.v6i1.3376.
- [3] H. Al-Rushdan, M. Shurman, S. H. Alnabelsi, and Q. Althebyan, "Zero-Day Attack Detection and Prevention in Software-Defined Networks," in *2019 International Arab Conference on Information Technology (ACIT)*, IEEE, Dec. 2019, pp. 278–282. doi: 10.1109/ACIT47987.2019.8991124.
- [4] S. Stat., M. Kom. Satriadi Putra Santika, "MENGENAL ZERO-DAY ATTACK, CELAH KEAMANAN YANG TIDAK TERLIHAT," BINUS UNIVERSITY SCHOOL OF COMPUTER SCIENCE.

- [5] Tushar Rakshe and Vishal Gonjari, "Anomaly based Network Intrusion Detection using Machine Learning Techniques," *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT)*, vol. 6, no. 5, May 2017.
- [6] S. Latif, F. F. Dola, MD. M. Afsar, I. Jahan Esha, and D. Nandi, "Investigation of Machine Learning Algorithms for Network Intrusion Detection," *International Journal of Information Engineering and Electronic Business*, vol. 14, no. 2, pp. 1–22, Apr. 2022, doi: 10.5815/ijieeb.2022.02.01.
- [7] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.
- [8] R. W. Shiddiq, N. Karna, and I. Dyah Irawati, "Optimizing Machine Learning-Based Network Intrusion Detection System with Oversampling, Feature Selection and Extraction," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)*, vol. 11, no. 2, pp. 225–237, 2025, doi: 10.26555/jiteki.v11i2.30675.
- [9] R. Kale, Z. Lu, K. W. Fok, and V. L. L. Thing, "A Hybrid Deep Learning Anomaly Detection Framework for Intrusion Detection," Dec. 2022, doi: 10.1109/BigDataSecurityHPSCIDS54978.2022.00034.
- [10] M. M. Issa, M. Aljanabi, and H. M. Muhialdeen, "Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations," *Journal of Intelligent Systems*, vol. 33, no. 1, Jun. 2024, doi: 10.1515/jisys-2023-0248.
- [11] O. Nwabuko, "An Overview of Research Study Designs in Quantitative Research Methodology," *American Journal of Medical and Clinical Research & Reviews*, vol. 03, no. 05, pp. 01–06, 2024, doi: 10.58372/2835-6276.1169.
- [12] H. Dermawan and A. Hasibuan, "Metode Penelitian Eksperimen: Prinsip, Prosedur, dan Aplikasi dalam Penelitian Ilmiah," *Factory Jurnal Industri, Manajemen dan Rekayasa Sistem Industri*, vol. 3, no. 2, pp. 47–50, May 2025, doi: 10.56211/factory.v3i2.729.
- [13] Zafar Iqbal Khan, Mohammad Mazhar Afzal, and Khurram Naim Shamsi, "A Comprehensive Study on CIC-IDS2017 Dataset for Intrusion Detection Systems," *International Research Journal on Advanced Engineering Hub (IRJAEH)*, vol. 2, no. 02, pp. 254–260, Feb. 2024, doi: 10.47392/IRJAEH.2024.0041.
- [14] H. Cevikalp, "High-dimensional data clustering by using local affine/convex hulls," *Pattern Recognit Lett*, vol. 128, pp. 427–432, Dec. 2019, doi: 10.1016/j.patrec.2019.10.007.
- [15] P. G. J. and N. K. V., "Google Colaboratory : Tool for Deep Learning and Machine Learning Applications," *Indian Journal of Computer Science*, vol. 6, no. 3–4, p. 23, Aug. 2021, doi: 10.17010/ijcs/2021/v6/i3-4/165408.