Journal of Information Technology and Computer Science (INTECOMS)
Volume 9 Nomor 5, Tahun 2026
e-ISSN : 2614-1574
p-ISSN : 2621-3249

MODEL MACHINE LEARNING UNTUK KLASIFIKASI ANOMALI SERANGAN DENIAL OF SERVICE (DOS) PADA INFRASTRUKTUR JARINGAN MENGGUNAKAN DATASET CIC IIOT 2025

MACHINE LEARNING MODEL FOR DENIAL OF SERVICE (DOS) ATTACK ANOMALY CLASSIFICATION IN NETWORK INFRASTRUCTURE USING THE CIC IIOT 2025 DATASET

Tri Swastiningsih[1], Rudi Kurniawan[2], Elmayati[3], Nelly Khairani Daulay[4]
Fakultas Ilmu Teknik, Program Studi Rekayasa Sistem Komputer, Universitas Bina Insan, Lubuklinggau[1,2,3,4]
triswastin@gmail.com[1], rudi.kurniawan@univbinainsan.ac.id[2], elmayati@gmail.com[3], daulaynelly14@gmail.com[4]

ABSTRACT

The development of the Industrial Internet of Things (IIoT) enhances industrial system efficiency but also increases the risk of cyberattacks—specifically Denial of Service (DoS) attacks—which can disrupt network service availability. This study aims to develop and evaluate machine learning models for classifying DoS attack anomalies within IIoT infrastructure using the CIC IIoT 2025 dataset. The dataset comprises normal (benign) traffic and various types of DoS attacks, such as TCP SYN Flood, UDP Flood, ICMP Flood, and MQTT Publish Flood. Data imbalance issues were addressed using the Synthetic Minority Over-sampling Technique (SMOTE). Three supervised learning algorithms were employed: Random Forest, XGBoost, and Support Vector Machine (SVM). Evaluation was conducted using metrics including accuracy, precision, recall, F1-score, confusion matrix, ROC-AUC, and K-Fold Cross-Validation. The results indicate that Random Forest and XGBoost achieved the highest accuracy at 97%, while SVM achieved 95%. Overall, the models demonstrated stable performance in detecting various DoS attack variants. This study contributes to the development of machine learning-based intrusion detection systems to enhance IIoT network security

Keywords: *IIoT, Denial of Service, Machine Learning, SMOTE.*

ABSTRAK

Perkembangan Industrial Internet of Things (IIoT) meningkatkan efisiensi sistem industri, namun juga meningkatkan risiko serangan siber, khususnya Denial of Service (DoS) yang dapat mengganggu ketersediaan layanan jaringan. Penelitian ini bertujuan untuk membangun dan mengevaluasi model machine learning dalam mengklasifikasikan anomali serangan DoS pada infrastruktur IIoT menggunakan dataset CIC IIoT 2025. Dataset ini memuat trafik normal (benign) serta berbagai jenis serangan DoS seperti TCP SYN Flood, UDP Flood, ICMP Flood, dan MQTT Publish Flood. Permasalahan ketidakseimbangan data ditangani menggunakan metode Synthetic Minority Over-sampling Technique (SMOTE). Tiga algoritma supervised learning digunakan, yaitu Random Forest, XGBoost, dan Support Vector Machine (SVM). Evaluasi dilakukan menggunakan metrik accuracy, precision, recall, F1-score, confusion matrix, ROC-AUC, serta K-Fold Cross Validation. Hasil penelitian menunjukkan bahwa Random Forest dan XGBoost memperoleh akurasi tertinggi sebesar 97%, sedangkan SVM memperoleh akurasi 95%. Secara keseluruhan, menunjukkan performa paling stabil dalam mendeteksi berbagai variasi serangan DoS. Random Forest Penelitian ini berkontribusi dalam pengembangan sistem deteksi intrusi berbasis machine learning untuk meningkatkan keamanan jaringan IIoT.

Kata Kunci: IIoT, Denial of Service, Machine Learning, SMOTE.

PENDAHULUAN

Perkembangan Industrial Internet of Things (IIoT) telah mentransformasi sistem industri konvensional menjadi lingkungan yang saling terhubung dan terotomatisasi [1]. Integrasi sensor, perangkat pintar, dan teknologi komunikasi memungkinkan pertukaran data secara real-time sehingga meningkatkan efisiensi operasional dan produktivitas industri [2][3]. Namun demikian, peningkatan konektivitas tersebut juga memperluas permukaan serangan (attack surface) dan meningkatkan risiko ancaman keamanan siber [4][5].

Salah satu ancaman paling signifikan pada lingkungan IIoT adalah serangan Denial of Service (DoS) [6][7]. Serangan ini bertujuan untuk mengganggu ketersediaan layanan dengan membanjiri sistem atau jaringan menggunakan trafik berlebih sehingga pengguna sah tidak dapat mengakses layanan. Pada sistem industri, gangguan akibat DoS dapat menyebabkan kerugian finansial, terhentinya proses produksi, bahkan risiko keselamatan kerja [8].

Sistem deteksi intrusi (Intrusion Detection System/ IDS) berbasis signature memiliki keterbatasan dalam mendeteksi serangan baru atau zero-day attack. Oleh karena itu, pendekatan berbasis *machine learning* menjadi solusi yang lebih adaptif karena mampu mempelajari pola trafik jaringan dan mengidentifikasi anomali secara otomatis [9]. Beberapa algoritma yang banyak digunakan dalam penelitian keamanan jaringan antara lain Random Forest, Support Vector Machine (SVM), serta metode boosting seperti XGBoost .

Permasalahan umum dalam dataset keamanan siber adalah ketidak seimbangan kelas (class imbalance), di mana distribusi data antara trafik normal dan serangan tidak seimbang. Kondisi ini dapat menyebabkan bias pada model prediksi. Salah satu teknik yang umum digunakan untuk mengatasi permasalahan tersebut adalah Synthetic Minority Over-sampling Technique (SMOTE) [10].

Penelitian ini bertujuan untuk membangun dan mengevaluasi model machine learning dalam mengklasifikasikan anomali serangan DoS pada infrastruktur IIoT menggunakan dataset CIC IIoT 2025. Tiga algoritma supervised learning, yaitu Random Forest, XGBoost, dan SVM, dibandingkan berdasarkan metrik evaluasi seperti accuracy, precision, recall, F1-score, ROC-AUC, serta K-Fold Cross Validation [11]. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem deteksi intrusi yang efektif untuk meningkatkan keamanan jaringan IIoT.

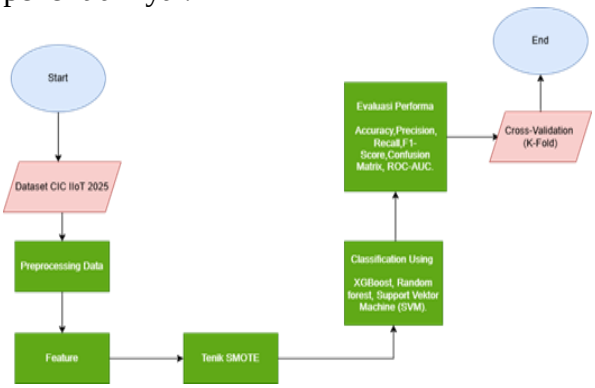
METODE

Penelitian ini menggunakan data sekunder berupa dataset CIC IIoT 2025 berformat CSV yang berisi trafik jaringan normal dan serangan DoS berlabel untuk kebutuhan klasifikasi, serta didukung studi pustaka dari jurnal dan literatur terkait.

Dataset yang digunakan adalah CIC IIoT 2025 yang diperoleh dari Canadian Institute for Cyber security dalam format CSV. Dataset ini berisi lalu lintas jaringan normal (benign) dan berbagai jenis serangan DoS seperti TCP SYN Flood, UDP Flood, ICMP Flood, dan MQTT Publish Flood. Data telah dilengkapi label kelas sehingga dapat digunakan untuk proses pelatihan dan pengujian model.

Metode Analisa

Pada penelitian ini digunakan metode analisis anomali untuk mendeteksi serangan pada infrastruktur jaringan. Metode ini mengidentifikasi aktivitas yang tidak wajar pada lalu lintas data, seperti lonjakan trafik secara tiba-tiba atau pengiriman paket berulang tanpa tujuan yang jelas. Berikut adalah gambar tahapan penelitiannya :



Gambar 1. Tahap Penelitian

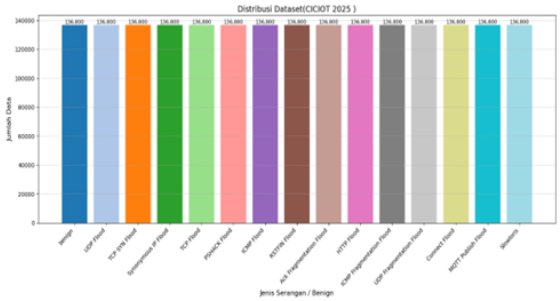
Gambar 1 menunjukkan alur penelitian dimulai dari penggunaan dataset CIC IIoT 2025, dilanjutkan dengan preprocessing dan pemilihan fitur, kemudian penyeimbangan data menggunakan teknik SMOTE. Data yang telah diproses digunakan untuk klasifikasi

dengan algoritma Random Forest, XGBoost, dan SVM.

Selanjutnya, performa model dievaluasi menggunakan metrik seperti accuracy, precision, recall, F1-score, confusion matrix, dan ROC-AUC, serta divalidasi menggunakan K-Fold Cross-Validation sebelum menghasilkan output akhir.

Pre-processing Data

Dataset serangan Denial of Service (DoS) di CIC IIoT 2025 terdiri dari 2.052.000 serangan. Berikut gambar distribusi dataset CICIOT 2025 :

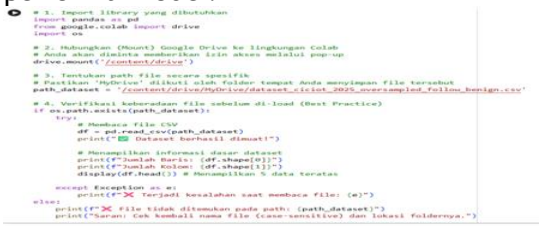


Gambar 2. Grafik Distribusi CICIOT 2025

Grafik diagram batang diatas menunjukkan distribusi 14 kelas pada dataset CIC IIoT 2025 yang telah melalui proses oversampling menggunakan SMOTE. Setiap kelas, termasuk Benign dan seluruh kategori Denial of Service (DoS) seperti TCP SYN Flood, UDP Flood, Slowloris, dan lainnya, memiliki jumlah data yang sama yaitu 136.800. Hal ini menunjukkan bahwa proses SMOTE berhasil menyeimbangkan data dengan menambahkan data sintetis pada kelas minoritas tanpa mengurangi jumlah data pada kelas mayoritas.

HASIL DAN PEMBAHASAN

Penelitian ini diimplementasikan menggunakan bahasa pemrograman Python melalui Google Colaboratory dengan memanfaatkan berbagai library pendukung. Tahapan penelitian meliputi pengunduhan dataset, preprocessing data, exploratory data analysis (EDA), proses klasifikasi menggunakan algoritma Random Forest, XGBoost, dan Support Vector Machine (SVM), serta evaluasi untuk mengukur performa model.



```
# 1. Import library yang dibutuhkan
import pandas as pd
from google.colab import drive
import os

# 2. Hubungkan (Mount) Google Drive ke lingkungan Colab
# Anda akan diminta memberikan izin akses melalui pop-up
drive.mount('/content/drive')

# 3. Tentukan path file secara spesifik
# Pastikan 'MyDrive' diikuti oleh folder tempat Anda menyimpan file tersebut
path_dataset = '/content/drive/MyDrive/dataset_ciciot_2025_oversampled_follow_benign.csv'

# 4. Verifikasi keberadaan file sebelum di-load (Best Practice)
if os.path.exists(path_dataset):
    try:
        # Membaca file CSV
        df = pd.read_csv(path_dataset)
        print("✅ Dataset berhasil dimuat!")

        # Menampilkan informasi dasar dataset
        print(f"Jumlah Baris: {df.shape[0]}")
        print(f"Jumlah Kolom: {df.shape[1]}")
        display(df.head()) # Menampilkan 5 data teratas

    except Exception as e:
        print(f"❌ Terjadi kesalahan saat membaca file: {e}")
else:
    print(f"❌ File tidak ditemukan pada path: {path_dataset}")
    print("Saran: Cek kembali nama file (case-sensitive) dan lokasi folernya.")
```

Gambar 3. Load Dataset

time-lation	network_ttl_avg	network_ttl_max	network_ttl_min	network_ttl_std_deviation	network_window-size_avg	network_window-size_max	network_window-size_min	network_window-size_std_deviation	label5
06059	62.800000	64.0	61.0	1.469694	1870.500000	3081.0	660.0	1210.500000	benign
16469	62.500000	64.0	61.0	1.500000	1870.500000	3081.0	660.0	1210.500000	benign
34312	61.571429	64.0	53.0	3.736199	2441.285714	4736.0	135.0	1813.237335	benign
12790	62.500000	64.0	61.0	1.500000	1870.500000	3081.0	660.0	1210.500000	benign
17764	62.800000	64.0	61.0	1.469694	2112.600000	3081.0	660.0	1186.042933	benign

Gambar 4. Hasil Load Dataset

Gambar tersebut menunjukkan **dataset statistik lalu lintas jaringan** yang berisi nilai TTL dan ukuran window seperti rata-rata, maksimum, minimum, serta standar deviasi. Setiap baris merepresentasikan satu aktivitas jaringan, dan kolom **label5** menunjukkan bahwa data tersebut termasuk **benign** atau lalu lintas jaringan normal.

Split Data

```
# ================================
# 5. SPLIT DATA (80:20)
# ================================
X_train, X_test, y_train, y_test = train_test_split(
    X, y_encoded,
    test_size=0.2,
    random_state=42,
    stratify=y_encoded
)
```

Gambar 5. Split Data

Gambar diatas menunjukkan proses split data dimana data dibagi menjadi data uji 80 % dan data latih 20%.

Pelatihan Model

Setelah melakukan spliting data langkah selanjutnya adalah melakukan elatihan menggunakan Random Frorest, XGBoost, Support Vektor Machine (SVM), untuk membandingkan hasil klasifikasi. Berikut gambar pelatihan model:

```
=== Melatih Model: Random Forest ===
Laporan Klasifikasi untuk Random Forest:
                          precision    recall  f1-score   support

Ack Fragmentation Flood       1.00      0.97      0.99     27360
          Connect Flood       1.00      1.00      1.00     27360
             HTTP Flood       0.99      0.98      0.99     27360
             ICMP Flood       1.00      0.97      0.98     27360
ICMP Fragmentation Flood      1.00      0.98      0.99     27360
      MQTT Publish Flood      1.00      1.00      1.00     27360
           PSHACK Flood       1.00      0.97      0.99     27360
           RSTFIN Flood       1.00      0.96      0.98     27360
              Slowloris       0.97      0.78      0.87     27360
    Synonymous IP Flood       1.00      0.98      0.99     27360
            TCP Flood         1.00      0.98      0.99     27360
        TCP SYN Flood         1.00      0.98      0.99     27360
            UDP Flood         1.00      0.98      0.99     27360
UDP Fragmentation Flood       1.00      0.98      0.99     27360
                benign        0.69      0.98      0.81     27360

              accuracy                            0.97    410400
             macro avg        0.98      0.97      0.97    410400
          weighted avg        0.98      0.97      0.97    410400
```

Gambar 6. Hasil Classification Report Random Forest

Gambar tersebut menampilkan **laporan klasifikasi dari model Random orest** yang digunakan untuk mendeteksi berbagai jenis serangan jaringan. Tabel tersebut menunjukkan nilai **precision, recall, f1-score, dan support** untuk setiap kelas serangan seperti Ack Fragmentation Flood, HTTP Flood, TCP Flood, hingga trafik normal (benign). Hasilnya menunjukkan bahwa sebagian besar kelas memiliki nilai evaluasi yang sangat tinggi mendekati 1.00), dengan **akurasi keseluruhan sebesar 0.97**, yang menandakan bahwa model Random Forest mampu mengklasifikasikan data dengan kinerja yang sangat baik.

```
=== Melatih Model: XGBoost ===
Laporan Klasifikasi untuk XGBoost:
                          precision    recall  f1-score   support

Ack Fragmentation Flood       1.00      0.97      0.98     27360
          Connect Flood       1.00      1.00      1.00     27360
             HTTP Flood       0.99      0.98      0.98     27360
             ICMP Flood       1.00      0.97      0.98     27360
ICMP Fragmentation Flood      1.00      0.99      0.99     27360
      MQTT Publish Flood      1.00      1.00      1.00     27360
           PSHACK Flood       1.00      0.97      0.99     27360
           RSTFIN Flood       1.00      0.96      0.98     27360
              Slowloris       0.96      0.78      0.86     27360
    Synonymous IP Flood       1.00      0.98      0.99     27360
            TCP Flood         1.00      0.98      0.99     27360
        TCP SYN Flood         1.00      0.98      0.99     27360
            UDP Flood         1.00      0.98      0.99     27360
UDP Fragmentation Flood       1.00      0.98      0.99     27360
                benign        0.69      0.98      0.81     27360

              accuracy                            0.97    410400
             macro avg        0.98      0.97      0.97    410400
          weighted avg        0.98      0.97      0.97    410400
```

Gambar 7. Hasil Classification Report XGBoost

Gambar 7 menunjukkan laporan klasifikasi dari model XGBoost dalam mendeteksi berbagai jenis serangan jaringan. Hasil evaluasi menunjukkan bahwa model memiliki performa yang sangat baik dengan nilai precision, recall, dan f1-score yang tinggi pada sebagian besar kelas, serta akurasi keseluruhan sebesar 0.97.

```
Laporan Klasifikasi untuk Linear_SVM:
                          precision    recall  f1-score   support

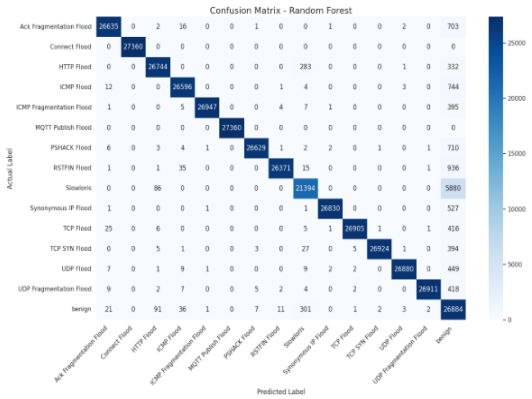
Ack Fragmentation Flood       1.00      0.96      0.98     27360
          Connect Flood       1.00      1.00      1.00     27360
             HTTP Flood       0.98      0.92      0.95     27360
             ICMP Flood       0.97      0.96      0.97     27360
ICMP Fragmentation Flood      1.00      0.98      0.99     27360
      MQTT Publish Flood      1.00      0.99      0.99     27360
           PSHACK Flood       1.00      0.95      0.97     27360
           RSTFIN Flood       1.00      0.95      0.97     27360
              Slowloris       0.81      0.77      0.79     27360
    Synonymous IP Flood       1.00      0.96      0.98     27360
            TCP Flood         1.00      0.97      0.98     27360
        TCP SYN Flood         1.00      0.97      0.98     27360
            UDP Flood         0.99      0.97      0.98     27360
UDP Fragmentation Flood       1.00      0.97      0.98     27360
                benign        0.63      0.90      0.74     27360

              accuracy                            0.95    410400
             macro avg        0.96      0.95      0.95    410400
          weighted avg        0.96      0.95      0.95    410400
```

Gambar 8. Classification Report SVM

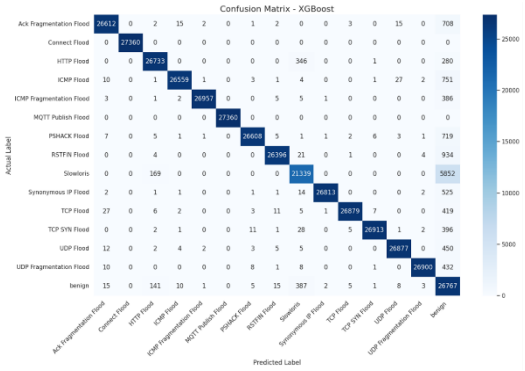
Gambar 8 menampilkan laporan klasifikasi dari model Linear SVM dalam mendeteksi berbagai jenis serangan jaringan. Hasil evaluasi menunjukkan bahwa model memiliki performa yang cukup baik dengan nilai precision, recall, dan f1-score yang tinggi pada sebagian besar kelas, serta akurasi keseluruhan sebesar 0.95.

Hasil Confusion Matrix



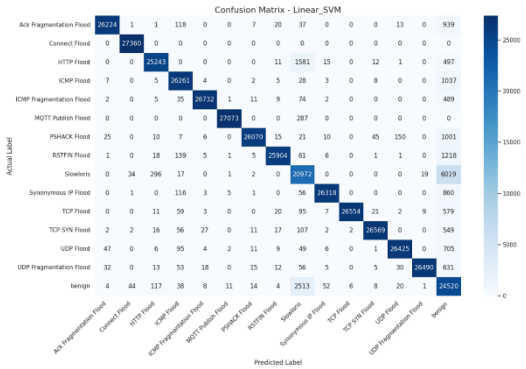
Gambar 9. Confusion Matrix Random Forest

Gambar di atas menunjukkan bahwa model Random Forest mampu mengklasifikasikan sebagian besar data dengan benar, terlihat dari dominasi nilai pada diagonal confusion matrix, meskipun masih terdapat sedikit kesalahan prediksi pada beberapa kelas.



Gambar 10. Confusion Matrix XGBoost

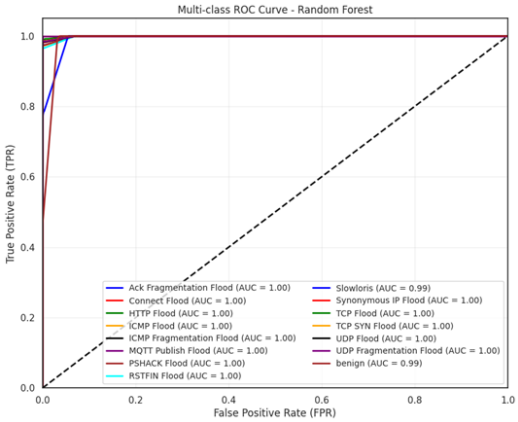
Confusion matrix di atas menunjukkan bahwa model XGBoost memiliki performa klasifikasi yang sangat baik, terlihat dari dominasi nilai pada diagonal utama yang menandakan prediksi benar. Sebagian besar jenis serangan dan kelas benign berhasil diklasifikasikan dengan akurat. Meskipun demikian, masih terdapat sedikit kesalahan prediksi, terutama pada kelas Slowloris yang kadang terklasifikasi sebagai benign serta beberapa jenis flood yang saling tertukar. Secara keseluruhan, model menunjukkan akurasi yang tinggi dengan tingkat kesalahan yang relatif kecil.



Gambar 11. Confusion Matrix Linear SVM

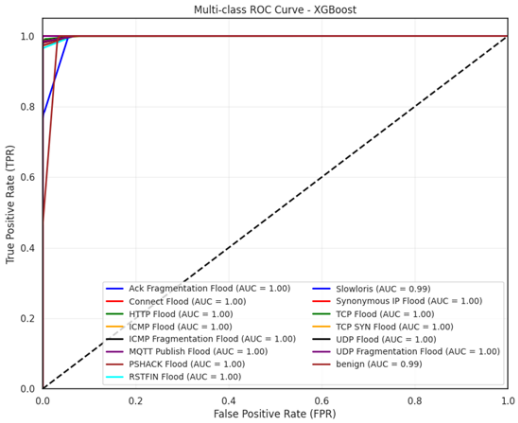
Confusion matrix model **Linear SVM** diatas menunjukkan bahwa model masih mampu mengklasifikasikan sebagian besar data dengan benar (terlihat dari nilai diagonal yang cukup besar), namun tingkat kesalahannya lebih tinggi dibandingkan model sebelumnya. Beberapa kelas seperti Connect Flood dan MQTT Publish Flood tetap terdeteksi dengan sangat baik, tetapi terdapat cukup banyak misklasifikasi pada kelas Slowloris yang sering diprediksi sebagai benign, serta kebingungan antar beberapa jenis flood seperti HTTP, ICMP, TCP, dan UDP. Selain itu, kelas benign juga cukup sering salah diklasifikasikan sebagai Slowloris. Secara umum, performa Linear SVM cukup baik, tetapi belum seakurat XGBoost karena jumlah kesalahan prediksinya lebih banyak.

Hasil Kurva ROC



Gambar 12. Hasil Grafik Kurva ROC Random Forest

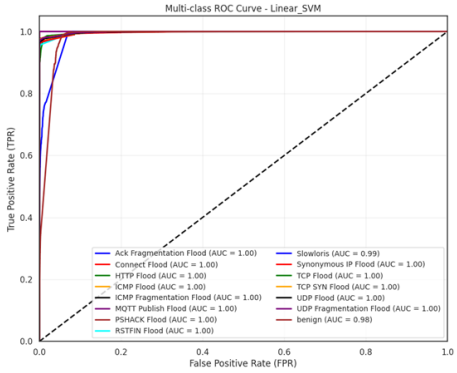
Gambar diatas menampilkan kurva ROC multi-class dari model Random Forest, di mana hampir semua kurva berada sangat dekat dengan sudut kiri atas grafik yang menunjukkan nilai True Positive Rate (TPR) tinggi dan False Positive Rate (FPR) rendah. Nilai AUC untuk hampir seluruh kelas mencapai 1.00, sementara beberapa seperti Slowloris dan benign sekitar 0.99, yang menandakan bahwa model memiliki kemampuan klasifikasi yang sangat tinggi dan hampir sempurna dalam membedakan setiap jenis serangan maupun trafik normal



Gambar 13. Hasil Grafik ROC XGBoost

Grafik tersebut menampilkan **kurva ROC multi-kelas** untuk model XGBoost, di mana sumbu X adalah False Positive Rate (FPR) dan sumbu Y adalah True Positive Rate (TPR). Hampir semua kelas serangan (seperti Ack Fragmentation Flood, HTTP Flood, ICMP Flood, dan lainnya) memiliki nilai AUC = 1.00, sedangkan beberapa kelas seperti Slowloris dan benign memiliki AUC sekitar 0.99.

Karena kurva tiap kelas berada sangat dekat dengan sudut kiri atas dan jauh di atas garis diagonal (garis tebakan acak), ini menunjukkan bahwa model memiliki performa klasifikasi yang sangat baik dan mampu membedakan tiap kelas dengan akurasi yang hampir sempurna.



Gambar 14. Hasil Grafik ROC Linear SVM

Grafik tersebut menunjukkan **kurva ROC multi-kelas untuk model Linear SVM**, dengan sumbu X sebagai False Positive Rate (FPR) dan sumbu Y sebagai True Positive Rate (TPR). Sebagian besar kelas serangan memiliki nilai AUC = 1.00, sementara beberapa kelas seperti *Slowloris* memiliki AUC sekitar 0.99 dan kelas benign sekitar 0.98. Kurva yang berada dekat dengan sudut kiri atas dan jauh di atas garis diagonal menandakan bahwa model Linear SVM memiliki kemampuan klasifikasi yang sangat tinggi dalam membedakan tiap jenis serangan dan trafik normal, meskipun performanya sedikit lebih rendah dibandingkan model dengan AUC sempurna di semua kelas.

SIMPULAN

Penelitian ini menunjukkan bahwa algoritma machine learning efektif dalam mengklasifikasikan anomali serangan DoS pada infrastruktur IIoT. Random Forest dan XGBoost mencapai akurasi tertinggi sebesar 97%, sedangkan SVM mencapai 95%. Random Forest menjadi model dengan performa paling stabil secara keseluruhan. Implementasi SMOTE terbukti membantu mengatasi ketidakseimbangan data. Penelitian ini dapat menjadi dasar pengembangan sistem deteksi intrusi berbasis machine learning pada lingkungan industri.

DAFTAR PUSTAKA

[1] A. Selay et al, “Internet of Things,” *Encycl. Wirel. Networks*, vol. 1, p. 664, 2020, doi: Encyclopedia of Wireless Networks.

[2] and S. L. L. Da Xu, W. He, “Internet of Things in Industries: A Survey,” *IEEE Trans. Ind. Informatics*, vol. 10, pp. 2233–2243, 2014.

[3] E. C. P. Neto et al, “CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment,” *Sensors*, vol. 23, 2023, doi: 10.3390/s23135941.

[4] and A. M. R. C. W. Kojansow, P. D. K. Manembu, “Using WebSocket communication,” *using WebSocket Commun.*, vol. 19, pp. 259–269, 2024.

[5] and T. W. H. Boyes, B. Hallaq, J. Cunningham, “The Industrial Internet of Things (IIoT): An Analysis Framework,” *Comput. Ind.*, vol. 101, pp. 1–12, 2018, doi: 10.1016/j.compind.2018.04.015.

[6] D. Chaitanya and G. Arindam, “Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation.”

[7] S. M. Mousavi and M. St-Hilaire, “Early Detection of DDoS Attacks Using Self-Organizing Maps,” *IEEE Int. Conf. Commun.*, 2015.

[8] A. Decision and C. Tree, “Identifikasi Serangan Denial of Service (DoS) di

Jaringan dengan Decision Tree," *Wahana Tridarma Perguru. Tinggi*, vol. 73, no. 2, pp. 13–29, 2021.

[9] and F. F. M. Mujiono, D. A. Larasati, M. Hemansyah, "Deteksi Anomali dalam Sistem Keamanan Jaringan Menggunakan Teknik Supervised Machine Learning," *J. Esensi Infokom*, vol. 1, pp. 65–69, 2025, doi: 10.55886/infokom.v9i1.971.

[10] and E. D. K. R. Arunika, L. Joni, "Perbandingan Model SARIMA, Exponential Smoothing, dan XGBoost untuk Prediksi," vol. 13, 2021.

[11] B. N. Nuzululnisa and H. Hairani, "Analisis Kinerja Model Random Forest dengan Teknik Manhattan-SMOTE pada Deteksi Fraud Transaksi Kartu Kredit Imbalance," pp. 65–71, 2025.

[12] D. F. and R. Rianti, "Dalam Lalu Lintas Jaringan Menggunakan Naive," vol. 5, pp. 140–148, 2023.