DEWANTARA. J. Tech., Vol. 06, No. 02 (2026), Hal. 168 - 184
E ISSN : 2776-6764
P ISSN : 2774-2032

Deteksi Serangan Man-In-The-Middle (MITM) Berbasis Machine Learning pada Dataset CIC IIOT 2025

Vera Deska-1[a*], Armanto-2[a], Elmayati-3[a]

[a]Studi Rekayasa Sistem Komputer, Universitas Bina Insan
Jl. Jendral Besar H. M Soeharto KM. 13 Kel. Lubuk Kupang Kec. Lubuklinggau Selatan I, Lubuklinggau, Indonesia

*Email : veradeska2727@gmail.com, armanto0204@gmail.com, elmayati@univbinainsan.ac.id,

Abstrak

Keamanan komunikasi data pada ekosistem *Industrial Internet of Things* (IIoT) menjadi sangat rentan terhadap serangan *Man-In-The-Middle* (MITM), di mana penyerang secara diam-diam menyadap atau memanipulasi lalu lintas data antar perangkat. Serangan ini sangat berbahaya dalam lingkungan industri karena dapat menyebabkan kesalahan instruksi pada mesin yang berujung pada kerusakan fisik. Penelitian ini bertujuan untuk mengimplementasikan model *machine learning* yang mampu mendeteksi keberadaan anomali MITM secara presisi. Dengan menggunakan dataset CIC IIoT 2025, penelitian ini menganalisis fitur-fitur jaringan yang paling representatif terhadap perilaku serangan *spoofing* dan *interception* untuk membangun sistem deteksi yang responsif. Metodologi penelitian ini mencakup tahapan preprocessing, penanganan ketidakseimbangan data, klasifikasi, dan evaluasi model. Pada tahap preprocessing dilakukan ekstraksi fitur, pembersihan data, dan normalisasi data. Jika terdapat ketidakseimbangan kelas, teknik SMOTE dapat digunakan untuk menyeimbangkan distribusi data. Selanjutnya, proses klasifikasi dilakukan menggunakan algoritma Decision Tree, Random Forest, dan Support Vector Machine (SVM). Evaluasi model dilakukan dengan metrik accuracy, precision, recall, f1-score, confusion matrix, serta AUC-ROC. Penggunaan dataset CIC IIoT 2025 memberikan keunggulan karena memuat data trafik yang relevan dengan protokol industri terbaru, sehingga hasil model memiliki validitas yang lebih tinggi. Hasil penelitian menunjukkan performa deteksi yang optimal dengan nilai *False Acceptance Rate* (FAR) yang rendah. Kontribusi penelitian ini diharapkan dapat menjadi fondasi dalam pengembangan sistem keamanan otonom yang mampu melindungi integritas data pada infrastruktur IIoT dari ancaman penyusupan pihak ketiga.

Kata Kunci: *Machine Learning, Man-In-The-Middle (MITM), Keamanan IIoT, Deteksi Anomali, CIC IIoT 2025.*

1. Latar Belakang

Perkembangan Industrial Internet of Things (IIoT) telah mendorong transformasi besar dalam sektor industri melalui integrasi perangkat seperti komputer industri, sensor, aktuator, programmable logic controller (PLC), serta sistem kontrol yang saling terhubung dalam satu ekosistem digital. Konektivitas ini memungkinkan proses produksi berlangsung secara otomatis, real-time, dan berbasis data, sehingga meningkatkan efisiensi operasional, produktivitas, serta akurasi pengambilan keputusan. Implementasi IIoT juga membuka peluang optimasi pemeliharaan prediktif (predictive

maintenance), pemantauan jarak jauh, hingga integrasi rantai pasok berbasis sistem cerdas [1]. Namun demikian, peningkatan konektivitas tersebut secara langsung memperluas attack surface jaringan industri. Semakin banyak perangkat yang terhubung, semakin besar pula potensi celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Oleh karena itu, aspek keamanan siber menjadi isu krusial dalam implementasi IIoT modern [2].

Secara karakteristik, jaringan IIoT memiliki perbedaan mendasar dibandingkan jaringan konvensional. Infrastruktur IIoT umumnya bersifat terdistribusi, heterogen, serta terdiri atas berbagai perangkat dengan kapasitas komputasi dan sumber daya terbatas [3]. Banyak perangkat industri dirancang dengan prioritas pada ketersediaan dan keandalan operasional, bukan pada mekanisme keamanan tingkat lanjut. Selain itu, penggunaan protokol komunikasi yang beragam dan terkadang belum diperbarui secara berkala menyebabkan sistem menjadi rentan terhadap eksploitasi. Kombinasi sifat tersebar, tidak seragam, dan keterbatasan sumber daya ini menjadikan lingkungan IIoT sebagai target potensial bagi berbagai ancaman siber [4].

Salah satu ancaman yang paling berbahaya dalam konteks jaringan industri adalah serangan Man-in-the-Middle (MITM). Pada serangan ini, pihak ketiga secara diam-diam menyusup di antara dua entitas yang sedang berkomunikasi untuk menyadap, memodifikasi, atau bahkan memanipulasi data tanpa sepengetahuan kedua belah pihak [5]. Dalam lingkungan industri, serangan MITM dapat berdampak serius, seperti perubahan parameter sistem kontrol, pencurian data produksi, hingga gangguan operasional yang berujung pada kerugian finansial besar. Oleh karena itu, penguatan sistem deteksi dan mitigasi berbasis teknologi cerdas menjadi sangat penting guna menjaga integritas, kerahasiaan, dan ketersediaan data dalam ekosistem IIoT. Serangan Man-in-the-middle pada lingkungan industri dapat menyebabkan konsekuensi yang cukup besar, mulai dari kebocoran data yang bersifat pribadi hingga gangguan pada fungsi sistem otomatis [6]. Seperti serangan ARP spoofing,peniruan identitas,dan IP spoofing sering-sering tidak terdekteksi oleh mekanisme keamanan tradisional karena pola lalu lintas yang menyerupai komunikasi normal [7].

Seiring dengan kemajuan teknologi,pegunaan Machine Learning semakin meluas dalam bidang keamanan jaringan. Tehnik ini memberikan kesempatan bagi sistem untuk mengenali pola lalu lintas dan membedakan antara aktivitas normal dan mencurigakan. Berbagai algoritma yang umum seperti random forest ,decision Tree, dan Support Vector Machine (SVM),menunjukan kinerja yang baik dalam mendeteksi serangan pada jaringan [8].

Dalam penelitian ini digunakan dataset CIC IIoT 2025 yang dikembangkan oleh Canadian Institute for Cybersecurity sebagai sumber data. Dataset ini memuat lalu lintas jaringan normal dan serangan siber, termasuk serangan Man-in-the-Middle (MITM), serta telah dilengkapi dengan label dan fitur jaringan yang lengkap sehingga sesuai untuk penelitian berbasis Machine Learning.

Berdasarkan uraian tersebut, penelitian mengenai deteksi serangan Man-in-the-Middle (MITM) pada jaringan Industrial Internet of Things menggunakan pendekatan Machine Learning perlu dilakukan sebagai upaya untuk meningkatkan keamanan jaringan IIoT di masa mendatang.

Hampir seluruh penelitian sebelumnya bersifat umum dalam hal deteks ancaman pada IIoT, atau hanya mencakup metode pembelajaran mesin untuk deteksi intrusi secara keseluruhan. Penelitian yang secara khusus membahas deteksi serangan Man-in-the-middle (MITM) pada jaringan IIoT dengan menggunakan dataset CIC IIoT 2025 masih sangat jarang, sehingga diperlukan kajian yang mendalam yang

memetakan karakteristik Man-in-the-middle (MITM) dan menilai efektif berbagai algoritma machine Learning untuk kasus ini [9].

Penelitian yang relevan, dapat diidentifikasi beberapa *research gap* yang memperkuat urgensi penelitian ini. Sebagaimana temuan terdahulu masih berfokus pada simulasi dan pengujian serangan MITM melalui teknik penetrasi seperti ARP poisoning dan penggunaan tool tertentu, sehingga kontribusinya lebih pada aspek eksploitasi dan analisis kerentanan, bukan pada pengembangan sistem deteksi otomatis [10]. Studi terdahulu menitikberatkan pada efektivitas serangan MITM menggunakan ARP spoofing, Ettercap, dan Hydra, serta membuktikan pentingnya implementasi HTTPS, namun belum mengkaji pendekatan berbasis *Machine Learning* untuk mendeteksi pola serangan secara cerdas dan prediktif [11].

Sementara itu, lainnya dalam *Machine Learning for Intrusion Detection in IIoT: A Comprehensive Review* hanya bersifat tinjauan literatur tanpa implementasi model empiris [12]. Studi lainnya membandingkan algoritma pada konteks IoT umum, bukan secara spesifik pada lingkungan IIoT serta belum berfokus pada jenis serangan MITM [13]. Selain itu, isu ketidakseimbangan kelas (class imbalance) yang memengaruhi performa model juga belum dianalisis secara mendalam dalam konteks dataset IIoT terbaru.

Dengan demikian, terdapat kesenjangan penelitian berupa belum adanya studi komparatif yang secara khusus mengembangkan dan menguji model *Machine Learning* untuk mendeteksi serangan MITM pada jaringan IIoT menggunakan dataset terkini yang merepresentasikan lalu lintas industri modern. Penelitian ini hadir untuk mengisi celah tersebut melalui perancangan dan evaluasi algoritma Random Forest, Decision Tree, dan SVM pada dataset CIC IIoT 2025 guna menghasilkan model deteksi yang lebih adaptif, akurat, dan relevan dengan kebutuhan keamanan IIoT saat ini.

Tujuan penelitian ini bertujuan untuk mengembangkan dan mengevaluasi model *Machine Learning* dalam mendeteksi serangan *Man-in-the-Middle (*MITM) pada jaringan *Industrial Internet of Things* (IIoT) menggunakan dataset CIC IIoT 2025, sehingga dapat meningkatkan keamanan dan keandalan jaringan IIoT. Kebaruan (*novelty*) penelitian ini terletak pada penggunaan dataset IIoT generasi terbaru yang merepresentasikan skenario industri aktual, analisis komparatif tiga algoritma klasifikasi populer untuk mengidentifikasi performa terbaik dalam mendeteksi MITM, serta evaluasi mendalam terhadap efektivitas model dalam meningkatkan sistem keamanan jaringan IIoT secara lebih akurat dan efisien.

2. Metodologi

Dalam studi ini, penulis menerapkan pendekatan penelitian kuantitatif, yang merupakan cara untuk mencari pengetahuan dengan menggunakan data yang sudah dikumpulkan sebagai alat untuk menganalisis informasi yang ingin dipahami. Pada bagian ini, metode kuantitatif digunakan untuk menyelidiki penerapan teknik machine learning dalam mengidentifikasi serangan terhadap keamanan jaringan, khususnya serangan *Man-in-the-Middle* (MITM) dan pada lingkungan *Industrial Internet of Things* (IIoT).

Penelitian ini menggunakan dataset CIC IIoT 2025 sebagai sumber data utama, yang mencakup lalu lintas jaringan normal serta berbagai jenis serangan yang telah diberi penanda. Semua data dianalisis melalui langkah-langkah pengolahan data dan pengembangan model *machine learning* dengan menerapkan berbagai algoritma seperti *Random Forest, Decision Tree,* dan *Support Vector Machine*.

Melalui pendekatan ini, tujuan penelitian adalah menciptakan model deteksi serangan yang tepat dengan mengevaluasi kinerja algoritma

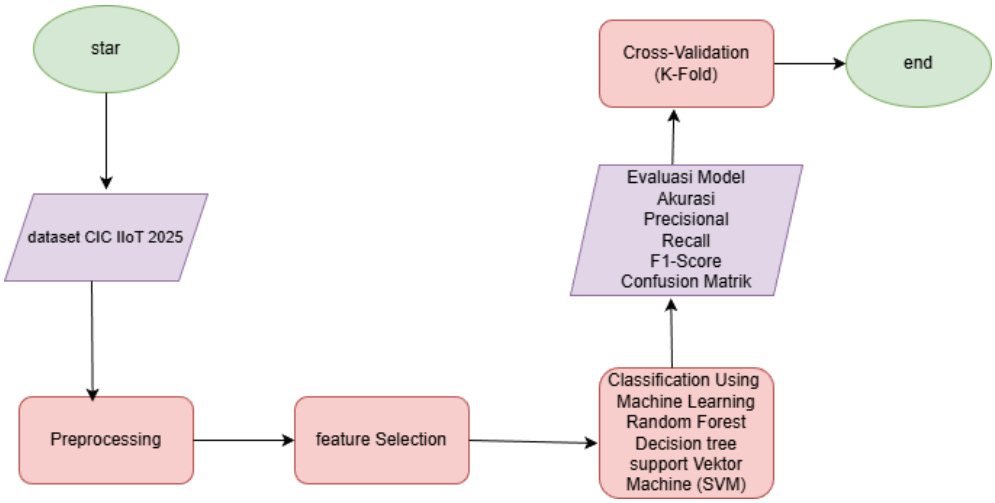
menggunakan analisis kuantitatif melalui metrik pengukuran seperti akurasi, presisi, recall, F1-score, dan ROC-AUC.

Penelitian ini dilaksanakan di Laboratorium Universitas Bina Insan Lubuklinggau. Waktu penelitian berlangsung dari September 2025 hingga Januari 2026, mencakup seluruh tahapan penelitian mulai dari penyusunan proposal, pengumpulan dan pengolahan data, pembangunan serta pelatihan model deteksi serangan MITM, evaluasi kinerja model, hingga penyusunan laporan akhir.

Pengumpulan informasi dalam penelitian ini dilakukan untuk memperoleh data yang relevan guna mencapai tujuan penelitian. Sumber data utama yang digunakan adalah dataset CIC IIoT 2025 yang tersedia dalam format CSV. Dataset ini memuat lalu lintas jaringan pada lingkungan *Industrial Internet of Things* (IIoT), yang mencakup aktivitas normal, komunikasi antarperangkat, serta berbagai jenis serangan, termasuk *Man-in-the-Middle* (MITM).

Data dalam dataset tersebut telah dilabeli untuk membedakan antara trafik normal dan trafik berbahaya sehingga dapat dimanfaatkan secara optimal dalam proses pelatihan dan pengujian model *machine learning*. Fitur yang tersedia meliputi alamat IP, port, protokol, waktu transmisi, ukuran paket, serta berbagai parameter statistik jaringan lainnya yang relevan untuk proses deteksi intrusi. Selain itu, dataset juga merekam interaksi jaringan secara rinci sehingga memungkinkan model pembelajaran mesin mengenali pola serangan secara lebih mendalam dan terarah berdasarkan label yang telah ditentukan.

Pengumpulan data dalam penelitian ini dilakukan melalui dua pendekatan, yaitu data sekunder dan metode pustaka. Data sekunder diperoleh langsung dari dataset CIC IIoT 2025 yang telah tersedia dan digunakan tanpa melakukan pengumpulan data lapangan secara langsung. Dataset ini dimanfaatkan untuk proses pelatihan (*training*) dan pengujian (*testing*) model deteksi serangan MITM. Sementara itu, metode pustaka dilakukan dengan mengkaji berbagai jurnal dan penelitian terdahulu yang berkaitan dengan keamanan jaringan, serangan MITM, ARP spoofing, IIoT, serta teknik *machine learning*. Kajian literatur ini bertujuan untuk memperkuat landasan teori, memahami karakteristik serangan, serta menentukan metode analisis dan algoritma yang paling sesuai untuk diterapkan dalam penelitian ini.



Gambar 1. *Langkah-Langkah proses Penelitian*

Metode analisis dalam penelitian ini diterapkan untuk memproses data, membangun model deteksi, serta mengevaluasi kinerja algoritma *Machine Learning* dalam mengenali serangan *Man-in-the-Middle* (MITM) pada jaringan

Industrial Internet of Things (IIoT). Proses analisis dilakukan secara sistematis dan terstruktur, dimulai dari tahap perencanaan hingga penarikan kesimpulan akhir. Tahap awal (*start*) diawali dengan penetapan tujuan penelitian, identifikasi permasalahan, penentuan sumber data, serta perancangan alur kerja penelitian secara menyeluruh. Selanjutnya, penelitian memanfaatkan dataset CIC IIoT 2025 sebagai sumber utama data yang berisi lalu lintas jaringan normal dan berbagai jenis serangan siber pada lingkungan industri. Dataset ini dipilih karena memiliki struktur data yang komprehensif dan variasi serangan yang relevan untuk menguji kemampuan sistem dalam mendeteksi pola serangan MITM.

Tahap berikutnya adalah *preprocessing*, yaitu proses pembersihan dan penyiapan data sebelum digunakan dalam pelatihan model. Pada tahap ini dilakukan penanganan nilai yang tidak valid, data duplikat, serta transformasi atau normalisasi fitur agar data berada dalam kondisi bersih, terstruktur, dan siap diolah. Setelah itu dilakukan *feature selection* untuk memilih fitur-fitur yang paling relevan sehingga dapat meningkatkan performa model, mempercepat proses pelatihan, serta mengurangi risiko *curse of dimensionality*.

Tahap inti penelitian adalah proses klasifikasi menggunakan algoritma *Machine Learning*, yaitu Random Forest, Decision Tree, dan Support Vector Machine (SVM). Random Forest digunakan sebagai metode *ensemble learning* berbasis banyak pohon keputusan untuk meningkatkan akurasi dan mengurangi *overfitting*. Decision Tree memodelkan proses klasifikasi dalam bentuk struktur pohon berbasis aturan, sedangkan SVM bekerja dengan mencari *hyperplane* optimal yang mampu memisahkan kelas normal dan kelas serangan secara maksimal. Setiap algoritma dilatih menggunakan data yang telah melalui tahap *preprocessing* dan *feature selection*.

Selanjutnya, dilakukan evaluasi model menggunakan metrik performa seperti akurasi, presisi, recall, F1-score, serta *confusion matrix* untuk mengetahui tingkat ketepatan dan kemampuan model dalam mendeteksi serangan MITM. Untuk memastikan konsistensi dan generalisasi model, diterapkan teknik *K-Fold Cross-Validation*, di mana dataset dibagi menjadi beberapa bagian dan proses pelatihan serta pengujian dilakukan secara bergantian. Tahap akhir (*end*) merupakan proses penarikan kesimpulan berdasarkan hasil evaluasi, penentuan model terbaik, serta penyusunan rekomendasi untuk pengembangan penelitian selanjutnya.

Metode pengujian dan pengelolahan data dalam penelitian ini dilakukan untuk memastikan bahwa model *Machine Learning* yang dibangun mampu mendeteksi serangan *Man-in-the-Middle* (MITM) pada jaringan IIoT secara akurat dan konsisten. Adapun metode pengujian dalam penelitian ini adalah Confusion Matrix. Confusion Matrix bertujuan menggambarkan performa dari sebuah model atau algoritma secara spesifik. Seperti yang terlihat pada tabel berikut:

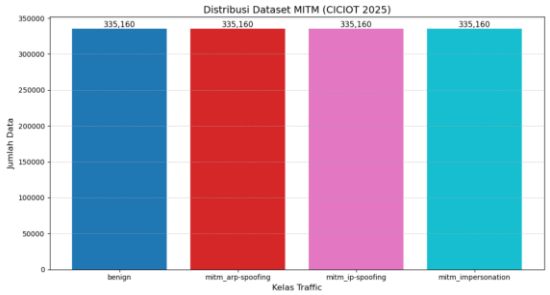
Tabel 1. Metode Pengujian Sistem

	Predicted Negative	Predicted Positive
Actual Negative	True Negative (TN)	False positive (FP)
Actual Positive	False Negative (FN)	True positive (TP)

Confusion Matrix digunakan untuk menggambarkan kinerja model klasifikasi berdasarkan empat komponen utama, yaitu *True Positive (TP), True Negative (TN), False Positive (FP), dan False Negative (FN). True Positive* merupakan data dengan kelas aktual positif yang berhasil diprediksi positif oleh model, sedangkan *True Negative* adalah data dengan kelas aktual negatif yang diprediksi negatif secara benar. *False Positive* terjadi ketika data aktual negatif namun diprediksi sebagai positif oleh model, sementara False Negative adalah data aktual positif tetapi

diprediksi negatif. Berdasarkan nilai-nilai tersebut, dapat dihitung beberapa metrik evaluasi untuk mengukur performa model, yaitu *Accuracy* yang dihitung dengan rumus (TP+TN)/Total untuk mengetahui proporsi prediksi yang benar secara keseluruhan, *Precision* dengan rumus TP/(FP+TP) untuk mengukur ketepatan prediksi positif, *Recall* dengan rumus TP/(FN+TP) untuk menilai kemampuan model mendeteksi kelas positif, serta F1-Score yang merupakan rata-rata harmonik antara Precision dan Recall dengan rumus 2*(*precision***recall*)/(*precision*+*recall*).

Pengelolaan data dilakukan sebagai berikut:



Gambar 2. Distribusi Data

Berdasarkan data grafik di atas dapat dilihat jumlah keseluhan dari data MITM dataset CIC IIoT2025 yang terdiri dari empat Kelas yaitu Benign sebesar : 335.160, mitm_arp-spoofing : 335.160 mitm_ip-spoofing: 335.160 Mitm_ Impersonation : 335.160.

3. Hasil dan Pembahasan

Dalam penelitian ini, implementasi dilakukan dengan menggunakan Bahasa pemrograman *python* dengan *google colaboratory*. Untuk menjalankan *script python* dibutuhkan library, karena *library* merupakan sekumpulan kode yang dilakukan beulang kali dalam program yang berbeda. Untuk mendapatkan hasil dalam penelitian ini diperlukan beberapa tahapan yang dilakukan dari pengumpulan data dengan pengunduhan dataset, tahap preprocessing data, tahap *ekploratory* data tahap klasifikasi dengan algoritma Random *Forest, decision tree, Support Vektor Machine (*SVM) dan evaluasi.

Load Dtaset

Tahap Awal yang dilakukan Adalah Load dataset CIC IIOT 2025 dapat dilihat pada gambar berikut.

```
# 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_MITM_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 foldernya.")
```

Gambar 3. Load Dataset

Tahap awal dalam penelitian ini adalah melakukan proses *load dataset* CIC IIoT 2025 ke dalam lingkungan Google Colab. Proses ini diawali dengan mengimpor pustaka yang dibutuhkan, yaitu *pandas* untuk pengolahan data serta *google.colab.drive* untuk mengakses file yang tersimpan di *Google Drive*. Selanjutnya, dilakukan proses *mounting Google Drive* agar sistem dapat membaca file dataset yang telah disimpan pada direktori tertentu. Setelah menentukan *path*

file secara spesifik, dilakukan verifikasi keberadaan file menggunakan fungsi os.path.exists() sebagai langkah *best practice* untuk menghindari kesalahan pembacaan data. Jika file ditemukan, dataset dibaca menggunakan fungsi pd.read_csv() dan disimpan ke dalam variabel *data frame*. Sistem kemudian menampilkan informasi dasar dataset seperti jumlah baris, jumlah kolom, serta lima data teratas untuk memastikan bahwa proses pemuatan data berjalan dengan baik. Tahapan ini penting sebagai langkah awal sebelum memasuki proses prapemrosesan dan analisis data lebih lanjut.

Hasil Load Dataset

Untuk hasil load dataset menggunakan data *frame* dapat dilihat pada gambar di bawah.

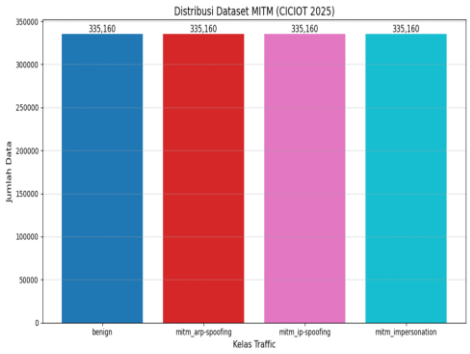
me	device_mac	label_full	label1	label2	label3	label4	timestamp	timestamp_start	timestamp_end	...	network_time-delta_std_deviation
ıter	28:87:ba:bd:c6:6c	benign_whole-network3	benign	benign	benign	benign	2025-09-09T14:09:40.400000Z_2025-09-09T14:09:4...	2025-09-09T14:09:40.400000Z	2025-09-09T14:09:41.400000Z	...	0.006059
ıter	28:87:ba:bd:c6:6c	benign_whole-network3	benign	benign	benign	benign	2025-09-09T14:09:41.400000Z_2025-09-09T14:09:4...	2025-09-09T14:09:41.400000Z	2025-09-09T14:09:42.400000Z	...	0.016469
ıter	28:87:ba:bd:c6:6c	benign_whole-network3	benign	benign	benign	benign	2025-09-09T14:09:42.400000Z_2025-09-09T14:09:4...	2025-09-09T14:09:42.400000Z	2025-09-09T14:09:43.400000Z	...	0.034312
ıter	28:87:ba:bd:c6:6c	benign_whole-network3	benign	benign	benign	benign	2025-09-09T14:09:43.400000Z_2025-09-09T14:09:4...	2025-09-09T14:09:43.400000Z	2025-09-09T14:09:44.400000Z	...	0.012790
ıter	28:87:ba:bd:c6:6c	benign_whole-network3	benign	benign	benign	benign	2025-09-09T14:09:44.400000Z_2025-09-09T14:09:4...	2025-09-09T14:09:44.400000Z	2025-09-09T14:09:45.400000Z	...	0.017764

olumns

Gambar 4. Hasil load Dataset

Gambar 4 menunjukkan hasil proses *load dataset* menggunakan struktur data frame, yang menampilkan beberapa kolom penting seperti *device_mac*, *label_full*, *label1*, *label2*, *label3*, *label4*, *timestamp*, *timestamp_start*, *timestamp_end*, serta *network_time_delta_std_deviation*.

Berdasarkan tampilan tersebut, dataset berhasil dimuat dengan baik ke dalam lingkungan analisis, ditandai dengan tersusunnya data dalam format tabular yang rapi dan terstruktur. Setiap baris merepresentasikan satu entri data dengan identitas perangkat (*device_mac*) yang sama, sementara kolom label menunjukkan kategori data, yaitu "benign" pada seluruh level pelabelan. Informasi waktu dicatat secara detail dalam format UTC pada kolom *timestamp*, *timestamp_start*, dan *timestamp_end*, yang memungkinkan analisis berbasis rentang waktu. Selain itu, terdapat nilai numerik pada kolom *network_time_delta_std_deviation* yang merepresentasikan variasi waktu jaringan, sehingga dapat digunakan sebagai salah satu fitur dalam proses analisis lebih lanjut, seperti deteksi anomali atau klasifikasi data jaringan. Secara keseluruhan, hasil *load dataset* ini menunjukkan bahwa data telah siap untuk tahap prapemrosesan dan analisis berikutnya. Distribusi data pada dataset yang digunakan dalam penelitian ini dapat dilihat pada gambar berikut.



Gambar 5. Distribusi Dataset Perkelas

Berdasarkan data grafik di atas dapat dilihat jumlah keseluhan dari data MITM dataset CIC IIoT2025 yang terdiri dari empat Kelas yaitu Benign sebesar : 335.160, mitm_arp-spoofing : 335.160 mitm_ip-spoofing : 335.160 Mitm_ Impersonation : 335.160 .

Data, berikut sudah melalui proses Oversampling (SMOTE) untuk menyeimbangkan data karna ada beberapa kategori mengalami ketidak seimbangan data, dengan menambahkan data sintesis pada kelas minoritas tanpa mengurangi kelas mayoritas.

Distribusi data pada dataset yang digunakan dalam penelitian ini dapat dilihat pada gambar berikut.

Pengujian Hasil Klasifikasi

Setelah melakukan proses pelatihan atau training, model ini akan evaluasi untuk melihat performa dari model yang telah dibangun, berikut ini evaluasi dari model.

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

            Benign       0.92      1.00      0.96    335160
 mitm_arp-spoofing       1.00      0.95      0.97    335160
  mitm_ip-spoofing       1.00      0.96      0.98    335160
Mitm_Impersonation       1.00      1.00      1.00    335160

          accuracy                           0.98   1340640
         macro avg       0.98      0.98      0.98   1340640
      weighted avg       0.98      0.98      0.98   1340640
```

Gambar 6. Classification Report Decision Tree

Berdasarkan hasil *classification report* pada pengujian model Decision Tree, dapat disimpulkan bahwa model menunjukkan kinerja yang sangat baik dalam mengklasifikasikan empat kelas serangan, yaitu Benign, mitm_arp-spoofing, mitm_ip-spoofing, dan Mitm_ Impersonation. Secara keseluruhan, model mencapai nilai akurasi sebesar 98%, yang menunjukkan bahwa sebagian besar data uji berhasil diklasifikasikan dengan benar dari total 1.340.640 sampel data.

Pada kelas Benign, model menghasilkan nilai *precision* sebesar 0,92, *recall* 1,00, dan *f1-score* 0,96, yang mengindikasikan bahwa seluruh data benign berhasil terdeteksi dengan sangat baik, meskipun masih terdapat sedikit kesalahan prediksi berupa *false positive*. Untuk kelas mitm_arp-spoofing, model menunjukkan performa yang sangat tinggi dengan *precision* 1,00, *recall* 0,95, dan *f1-score* 0,97, yang berarti hampir seluruh serangan ARP spoofing dapat dikenali dengan tingkat kesalahan yang sangat rendah. Selanjutnya, pada kelas mitm_ip-spoofing, model juga memperlihatkan kinerja yang sangat optimal dengan *precision* 1,00, *recall* 0,96, dan *f1-score* 0,98, menandakan kemampuan model yang kuat dalam mendeteksi serangan IP spoofing.

Kinerja terbaik ditunjukkan pada kelas Mitm_Impersonation, di mana model mencapai nilai *precision*, *recall*, dan *f1-score* masing-masing sebesar 1,00, yang berarti seluruh data pada kelas ini berhasil diklasifikasikan dengan sempurna tanpa kesalahan. Selain itu, nilai macro average dan weighted average untuk *precision*, *recall*, dan *f1-score* masing-masing sebesar 0,98, menunjukkan bahwa model Decision Tree memiliki performa yang konsisten dan seimbang pada seluruh kelas, meskipun dataset yang digunakan memiliki jumlah data yang besar. Dengan demikian, hasil ini membuktikan bahwa algoritma Decision *Tree* sangat efektif dan andal untuk digunakan dalam proses klasifikasi serangan *Man-in-the-Middle (MitM)* pada dataset yang digunakan dalam penelitian ini.

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

            Benign       0.92      1.00      0.96    335160
 mitm_arp-spoofing       1.00      0.95      0.97    335160
  mitm_ip-spoofing       1.00      0.96      0.98    335160
Mitm_Impersonation       1.00      1.00      1.00    335160

          accuracy                           0.98   1340640
         macro avg       0.98      0.98      0.98   1340640
      weighted avg       0.98      0.98      0.98   1340640
```

Gambar 7. Classification Report Random Forest

Berdasarkan hasil pengujian model *Random Forest* yang disajikan pada laporan klasifikasi, terlihat bahwa model menunjukkan performa yang sangat impresif dalam mengklasifikasikan empat jenis trafik jaringan, yaitu *Benign*, *mitm_arp-spoofing*, *mitm_ip-spoofing*, dan *Mitm_Impersonation*. Secara keseluruhan, model mencapai nilai akurasi sebesar 0,98 (98%) dari total data pengujian sebanyak 1.340.640 sampel. Hal ini menunjukkan bahwa algoritma *Random Forest* mampu

membedakan karakteristik trafik normal dan serangan *Man-in-the-Middle* (MitM) dengan tingkat kesalahan yang sangat minim.

Pada rincian per kelas, kategori Mitm_Impersonation berhasil diklasifikasikan dengan sempurna, ditunjukkan oleh nilai *precision*, *recall*, dan *f1-score* yang mencapai 1,00. Untuk kelas Benign, model memperoleh nilai *recall* maksimal sebesar 1,00, yang mengindikasikan bahwa tidak ada trafik normal yang terlewatkan oleh sistem (tidak ada *false negative* pada trafik normal), meskipun nilai *precision* sebesar 0,92 menunjukkan adanya sedikit data serangan yang terdeteksi sebagai trafik normal (*false positive*). Sebaliknya, pada kelas mitm_arp-spoofing dan mitm_ip-spoofing, model mencatatkan nilai *precision* sempurna (1,00), yang berarti setiap prediksi serangan pada kategori ini terbukti akurat, dengan nilai *recall* yang tetap sangat tinggi di angka 0,95 dan 0,96.

Konsistensi performa model juga diperkuat oleh nilai macro average dan weighted average yang berada di angka 0,98 untuk semua metrik utama. Mengingat jumlah dukungan data (*support*) yang terdistribusi secara merata (seimbang) sebesar 335.160 sampel untuk setiap kelas, hasil ini menunjukkan bahwa model memiliki kemampuan generalisasi yang sangat stabil dan tidak mengalami bias terhadap salah satu kelas tertentu. Dengan demikian, penggunaan model *Random Forest* dalam penelitian ini terbukti efektif dalam mendeteksi berbagai jenis serangan siber berbasis MitM dengan tingkat keandalan yang tinggi.

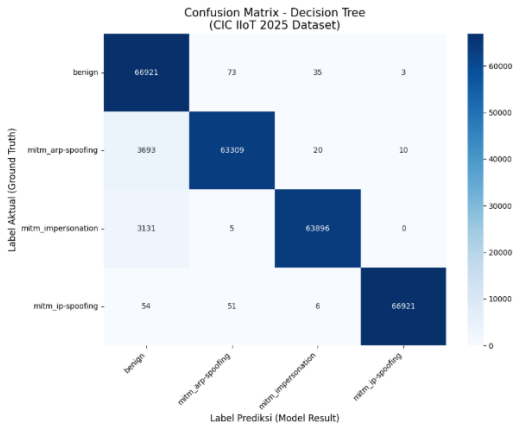
```
Melatih SVM (LinearSVC)...
Selesai! Laporan Klasifikasi SVM (LinearSVC):
                   precision    recall  f1-score   support

           benign       0.81      0.93      0.86     67032
 mitm_arp-spoofing       0.91      0.85      0.88     67032
mitm_impersonation       0.99      0.92      0.96     67032
  mitm_ip-spoofing       1.00      0.99      0.99     67032

          accuracy                           0.92    268128
         macro avg       0.93      0.92      0.92    268128
      weighted avg       0.93      0.92      0.92    268128
```

Gambar 8. Classification SVM

Berdasarkan hasil pengujian menggunakan algoritma *Support Vector Machine* (LinearSVC) terhadap dataset serangan *Man-in-the-Middle* (MitM), model menunjukkan performa yang solid dengan nilai akurasi keseluruhan sebesar 0,92 (92%) dari total 268.128 sampel data. Hasil ini mengindikasikan bahwa model memiliki kemampuan yang baik dalam mengklasifikasikan trafik jaringan ke dalam empat kategori utama, yaitu *benign*, *mitm_arp-spoofing*, *mitm_impersonation*, dan *mitm_ip-spoofing*. Stabilitas model juga terlihat dari nilai *macro average* dan *weighted average* pada metrik *f1-score* yang konsisten berada di angka 0,92.

Secara mendalam, model SVM mencapai performa tertinggi pada klasifikasi mitm_ip-spoofing dengan nilai *precision* mencapai 1,00 dan *recall* sebesar 0,99, menghasilkan *f1-score* hampir sempurna sebesar 0,99. Hal ini menunjukkan bahwa karakteristik serangan *IP spoofing* sangat mudah dikenali secara linier oleh model ini. Kategori *mitm_impersonation* juga menunjukkan hasil yang sangat baik dengan *f1-score* 0,96. Namun, terdapat sedikit penurunan performa pada kelas *mitm_arp-spoofing* dan *benign*. Kategori trafik *benign* (normal) mencatatkan nilai *precision* terendah sebesar 0,81, yang mengindikasikan adanya sejumlah trafik serangan yang terdeteksi sebagai trafik normal (*false positive*), meskipun nilai *recall* tetap tinggi di angka 0,93.

Penggunaan dataset dengan jumlah dukungan (*support*) yang seimbang, yakni 67.032 sampel untuk setiap kelas, memastikan bahwa evaluasi ini objektif dan tidak bias terhadap kelas mayoritas. Secara keseluruhan, meskipun terdapat variasi performa antar kelas, LinearSVC terbukti efektif sebagai metode deteksi serangan MitM, terutama dalam membedakan serangan manipulasi IP dan impersonasi dengan tingkat akurasi yang dapat diandalkan untuk kebutuhan keamanan jaringan.

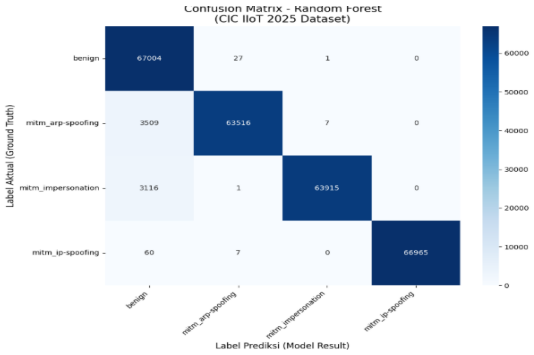


Gamber 9. Confusion Matrix Decision Tree

Berdasarkan data mentah dari *confusion matrix* tersebut, kita dapat menghitung performa spesifik model untuk mendukung analisis kualitatif sebelumnya. Dari total 268.128 sampel pengujian (67.032 sampel per kelas), model *Decision Tree* berhasil memprediksi 261.047 sampel secara benar (diagonal utama). Hal ini menghasilkan tingkat akurasi klasifikasi sebesar 97,36%.

Secara lebih mendalam, dapat diamati distribusi kesalahan (misklasifikasi) sebagai berikut: 1) Akurasi Tertinggi: Kelas benign dan mitm_ip-spoofing mencatatkan performa tertinggi dengan tingkat keberhasilan identifikasi sebesar 99,83% (66.921 dari 67.032 sampel). 2) Tingkat False Negative (FN): Kelas mitm_arp-spoofing memiliki tingkat *False Negative* tertinggi, di mana sebesar 5,51% (3.693 sampel) dari total serangan tersebut gagal terdeteksi dan dianggap sebagai trafik normal (*benign*). 3) Tingkat False Positive (FP): Dari sisi trafik benign, model memiliki tingkat *False Positive* yang sangat rendah, yakni hanya 0,16%, yang berarti sangat jarang trafik normal salah diidentifikasi sebagai serangan.

Data ini menunjukkan bahwa meskipun model sangat cerdas dalam mengenali serangan, tantangan utama terletak pada sekitar 5% hingga 6% serangan *ARP spoofing* dan *impersonation* yang masih memiliki kemiripan pola dengan trafik normal (benign) di lingkungan IIoT tersebut.



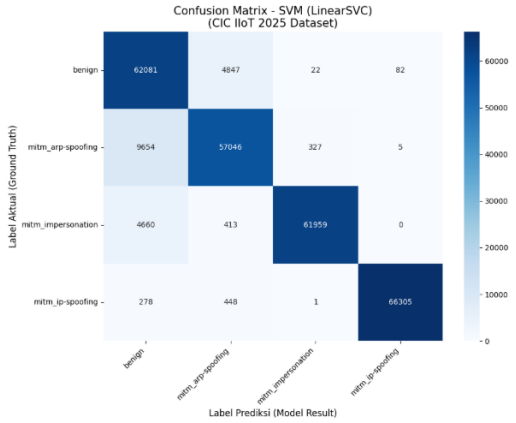
Gambar 10. confusion Matrix Random Forest

Berdasarkan data mentah dari confusion matrix model Random Forest, dapat dilakukan perhitungan performa spesifik guna mendukung analisis kualitatif sebelumnya. Dari total 268.128 sampel pengujian (67.032 sampel per kelas), model Random Forest berhasil memprediksi 261.400 sampel secara benar yang tersebar pada diagonal utama matriks. Pencapaian ini menghasilkan tingkat akurasi klasifikasi keseluruhan sebesar 97,49%.

Secara lebih mendalam, distribusi keberhasilan dan kesalahan (misklasifikasi) dapat diamati sebagai berikut: 2) Akurasi Tertinggi: Kelas benign dan mitm_ip-spoofing mencatatkan tingkat keberhasilan identifikasi tertinggi, masing-masing sebesar 67.004 dan 66.965 sampel dari total 67.032 data per kelas. 2) Tingkat False *Negative* (FN): Kelas mitm_arp-spoofing memiliki tingkat False Negative tertinggi, di mana sebesar 5,23% (3.509 sampel) dari total serangan tersebut gagal terdeteksi dan diklasifikasikan secara salah sebagai trafik normal (*benign*). 3) Tingkat *False Positive* (FP): Dari sisi trafik benign, model menunjukkan performa yang sangat luar biasa dengan tingkat *False Positive* yang jauh lebih rendah dari *Decision Tree*, yaitu hanya 0,04% (28 sampel), yang berarti hampir tidak ada trafik normal yang salah diidentifikasi sebagai serangan.

Data ini menunjukkan bahwa meskipun model *Random Forest* sangat akurat dalam mengenali pola serangan, tantangan utama tetap terletak pada kelas *mitm_arp-spoofing dan mitm_impersonation* (dengan 3.116

sampel yang terdeteksi sebagai *benign*). Hal ini mengindikasikan adanya kemiripan karakteristik fitur antara serangan manipulasi tersebut dengan trafik normal di lingkungan IIoT yang digunakan dalam penelitian ini.



Gambar 11. Confusion Matrix SVM

Berdasarkan data mentah dari *confusion matrix* model SVM (LinearSVC), kita dapat menghitung performa spesifik model untuk mendukung analisis kualitatif sebelumnya. Dari total 268.128 sampel pengujian (67.032 sampel per kelas), model SVM berhasil memprediksi 247.391 sampel secara benar (diagonal utama). Hal ini menghasilkan tingkat akurasi klasifikasi sebesar 92,27%.

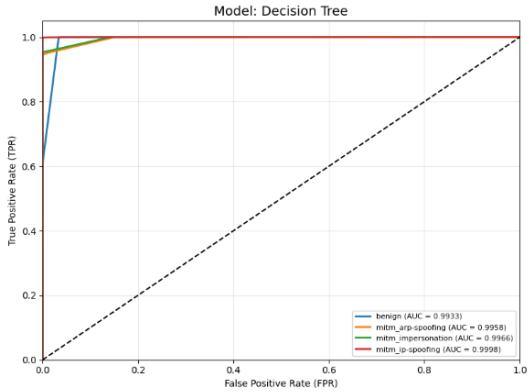
Secara lebih mendalam, dapat diamati distribusi kesalahan (misklasifikasi) sebagai berikut: 1) Akurasi Tertinggi: Kelas mitm_ip-spoofing mencatatkan performa tertinggi dengan tingkat keberhasilan identifikasi sebesar 98,92% (66.305 dari 67.032 sampel).

2) Tingkat False Negative (FN): Kelas mitm_arp-spoofing memiliki tingkat *False Negative* tertinggi dibandingkan kelas lainnya, di mana sebesar 14,40% (9.654 sampel) dari total serangan tersebut gagal terdeteksi dan dianggap sebagai trafik normal (*benign*). 3) Tingkat False Positive (FP): Dari sisi trafik benign, model memiliki tingkat *False Positive* sebesar 7,38%, di mana terdapat 4.951 sampel trafik normal yang salah diidentifikasi sebagai serangan (4.847 sebagai *arp-spoofing*, 22 sebagai *impersonation*, dan 82 sebagai *ip-spoofing*).

Data ini menunjukkan bahwa meskipun model SVM cukup handal dalam mengenali serangan *IP-spoofing*, tantangan utama terletak pada tingginya angka misklasifikasi pada serangan *ARP-spoofing* dan *impersonation* yang terdeteksi sebagai trafik normal. Hal ini mengindikasikan bahwa batas pemisah linier pada model LinearSVC kurang optimal dalam membedakan pola serangan tersebut dibandingkan dengan model berbasis pohon keputusan (*Decision Tree*).

Kurva ROC

Hasil dari kurva *ROC* dari hasil pelatihan dapat dilihat pada gambar berikut ini.

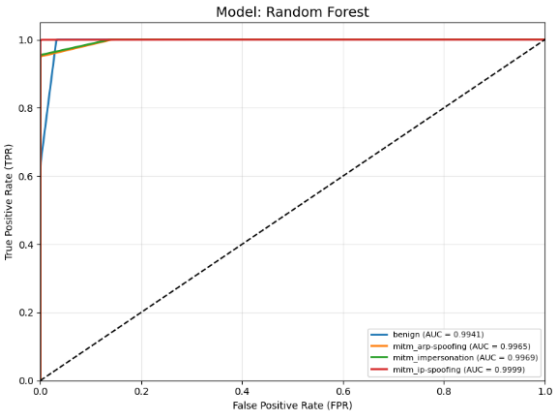


Gambar 12. KURVA ROC Dicision Tree

Visualisasi kurva *Receiver Operating Characteristic* (ROC) pada Gambar di atas menunjukkan performa diskriminasi yang sangat superior dari model *Decision Tree* dalam mengklasifikasikan trafik jaringan. Kualitas model ini dibuktikan dengan posisi seluruh kurva yang menempel mendekati sudut kiri atas grafik, yang mengindikasikan nilai *True Positive Rate* (TPR) yang tinggi dengan *False Positive Rate* (FPR) yang sangat rendah. Berdasarkan nilai *Area Under the Curve* (AUC), kategori mitm_ip-spoofing mencatatkan nilai tertinggi sebesar 0,9998, diikuti oleh mitm_impersonation sebesar 0,9966, dan mitm_arp-spoofing sebesar 0,9958. Nilai AUC yang mendekati angka sempurna (1,00) ini menegaskan bahwa

model memiliki pemisah probabilitas yang sangat tajam antara kategori serangan tersebut dengan kategori lainnya.

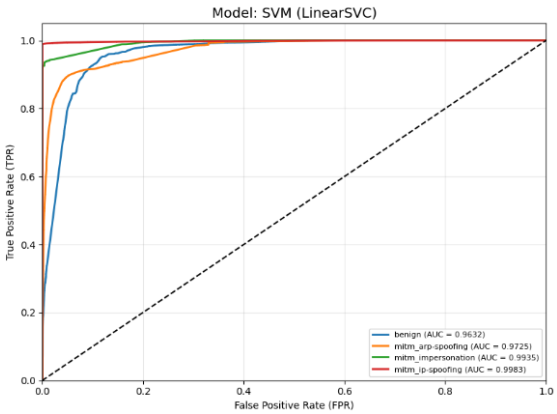
Sementara itu, untuk kategori benign (normal), model juga menunjukkan performa yang sangat kuat dengan nilai AUC sebesar 0,9933. Meskipun nilai ini merupakan yang paling rendah di antara kelas lainnya, angka tersebut tetap menunjukkan reliabilitas yang sangat tinggi dalam membedakan trafik normal dari ancaman serangan. Secara keseluruhan, karakteristik kurva ROC yang konsisten di atas garis diagonal (garis putus-putus) untuk semua kelas membuktikan bahwa algoritma *Decision Tree* sangat efektif dan stabil untuk digunakan sebagai mekanisme deteksi intrusi dalam ekosistem IIoT, karena mampu mempertahankan tingkat deteksi yang maksimal dengan meminimalisir kesalahan identifikasi.



Gambar 13. KURVA ROC Random Forest

Visualisasi kurva *Receiver Operating Characteristic* (ROC) pada gambar di atas menunjukkan kemampuan diskriminasi yang sangat luar biasa dari model *Random Forest* dalam mengklasifikasikan trafik jaringan pada dataset CIC IIoT 2025. Karakteristik kurva yang menempel sangat dekat dengan sudut kiri atas grafik mengindikasikan bahwa model mampu mencapai nilai *True Positive Rate* (TPR) yang maksimal dengan tingkat *False Positive Rate* (FPR) yang mendekati nol. Hal ini dipertegas oleh nilai *Area Under the Curve* (AUC) yang hampir sempurna untuk seluruh kategori, di mana kelas mitm_ip-spoofing mencatatkan nilai AUC tertinggi sebesar 0,9999, disusul oleh mitm_impersonation sebesar 0,9969, dan mitm_arp-spoofing sebesar 0,9965.

Selain pada kelas serangan, model juga menunjukkan reliabilitas yang sangat tinggi dalam mengidentifikasi trafik benign (normal) dengan nilai AUC sebesar 0,9941. Nilai AUC yang secara konsisten berada di atas 0,99 untuk semua kelas menunjukkan bahwa model memiliki ambang batas keputusan yang sangat stabil dan efektif dalam memisahkan pola trafik normal dari berbagai variasi serangan *Man-in-the-Middle*. Secara keseluruhan, hasil kurva ROC ini memberikan validasi visual yang kuat bahwa algoritma *Random Forest* memiliki performa deteksi intrusi yang sangat optimal dan dapat diandalkan untuk implementasi keamanan pada infrastruktur IIoT.



Gambar 14. Hasil KURVA ROC Dari SVM

Visualisasi kurva *Receiver Operating Characteristic* (ROC) untuk model SVM (LinearSVC) pada Gambar di atas menunjukkan kemampuan klasifikasi yang sangat kuat dalam membedakan berbagai jenis serangan *Man-in-the-Middle* (MitM). Seluruh kurva untuk setiap kelas berada jauh di atas garis diagonal referensi, yang secara visual mengonfirmasi bahwa model memiliki performa diskriminasi yang jauh lebih baik daripada klasifikasi acak. Hal ini dipertegas oleh nilai *Area Under the Curve* (AUC) yang tinggi untuk semua kategori, dengan skor tertinggi dicapai oleh kelas mitm_ip-spoofing sebesar 0,9983, diikuti

oleh mitm_impersonation sebesar 0,9935. Nilai AUC yang mendekati angka sempurna ini menunjukkan bahwa model sangat efektif dalam memisahkan probabilitas antara trafik serangan tersebut dengan kategori lainnya.

Meskipun menunjukkan performa yang solid secara keseluruhan, kurva untuk kategori benign dan mitm_arp-spoofing menunjukkan lengkungan yang sedikit lebih rendah dibandingkan dua kelas lainnya, dengan nilai AUC masing-masing sebesar 0,9632 dan 0,9725. Karakteristik kurva ini mengindikasikan bahwa model SVM (LinearSVC) memerlukan *False Positive Rate* (FPR) yang sedikit lebih tinggi untuk mencapai *True Positive Rate* (TPR) yang maksimal pada kedua kelas tersebut dibandingkan dengan serangan *IP-spoofing*. Secara umum, pencapaian nilai AUC di atas 0,96 untuk seluruh kategori trafik memberikan validasi bahwa pendekatan linier pada model SVM ini sangat handal dan memiliki tingkat kepercayaan yang tinggi dalam mendeteksi intrusi di jaringan IioT.

Hasil pengujian menunjukkan bahwa algoritma berbasis *supervised learning* mampu memberikan performa deteksi yang sangat tinggi pada dataset CIC IIoT 2025, khususnya untuk klasifikasi serangan Man-in-the-Middle (MitM). Pendekatan *supervised learning* sendiri merupakan metode pembelajaran mesin yang memanfaatkan data berlabel untuk membangun model prediktif, sehingga sangat sesuai digunakan dalam konteks deteksi intrusi yang telah memiliki kategori serangan yang jelas [14]. Hal ini sejalan dengan penelitian Rakhmadi Rahman dkk. yang menegaskan bahwa serangan MITM seperti ARP spoofing dan IP *spoofing* memiliki pola komunikasi jaringan tertentu yang dapat diidentifikasi melalui analisis lalu lintas [15]. Dengan memanfaatkan fitur-fitur statistik jaringan serta proses *oversampling* (SMOTE) untuk mengatasi ketidakseimbangan kelas, model *Decision Tree* dan *Random Forest* mampu mencapai akurasi di atas 97%, sedangkan SVM menunjukkan performa 92%. Temuan ini mengindikasikan bahwa pola serangan MitM pada lingkungan IIoT memiliki karakteristik yang cukup terstruktur sehingga efektif dipelajari oleh algoritma klasifikasi berbasis pohon maupun pemisah hiperbidang.

Secara teoritis, serangan Man-in-the-Middle terjadi ketika penyerang menyisipkan diri di antara dua pihak yang berkomunikasi untuk mencuri atau memanipulasi data tanpa diketahui oleh korban. Menurut Ajiginni, IP spoofing dan teknik impersonation memanfaatkan pemalsuan identitas alamat IP untuk mengelabui sistem keamanan jaringan, sehingga diperlukan pendekatan berbasis pembelajaran mesin seperti Multilayer Perceptron atau model klasifikasi lainnya untuk mengidentifikasi anomali pola komunikasi [16]. Dalam konteks penelitian ini, performa tinggi pada kelas mitm_ip-spoofing dan mitm_impersonation (AUC mendekati 1,00) menunjukkan bahwa model berhasil menangkap karakteristik statistik dari manipulasi paket data tersebut. Nilai AUC yang sangat tinggi pada *Random Forest* dan *Decision Tree* memperlihatkan kemampuan diskriminasi yang hampir sempurna dalam membedakan trafik normal dan serangan, yang secara praktis sangat penting dalam sistem deteksi intrusi berbasis IIoT.

Keunggulan model Random Forest dibandingkan SVM dalam penelitian ini juga dapat dijelaskan secara konseptual. *Random Forest* merupakan metode *ensemble learning* yang menggabungkan banyak pohon keputusan untuk meningkatkan stabilitas dan mengurangi *overfitting*. Dalam lingkungan Industrial *Internet of Things* (IIoT), lalu lintas jaringan cenderung kompleks dan memiliki variasi pola yang tinggi akibat interaksi perangkat industri secara real-time. Adi dan Ichsan menegaskan bahwa penerapan IIoT memberikan keuntungan ekonomi yang signifikan, namun juga meningkatkan risiko keamanan siber karena konektivitas yang luas [17]. Oleh karena itu, model yang

mampu menangkap hubungan non-linier seperti Random Forest menjadi lebih unggul dibandingkan model linier seperti LinearSVC, yang pada hasil penelitian ini menunjukkan tingkat *false negative* lebih tinggi pada serangan ARP *spoofing*. Hal ini mengindikasikan bahwa pola serangan tertentu mungkin tidak sepenuhnya dapat dipisahkan secara linier.

Implementasi penelitian ini menggunakan bahasa pemrograman Python di Google Colaboratory, yang mendukung efisiensi komputasi dan integrasi berbagai pustaka *machine learning*. Penggunaan Python dalam konteks analisis data dan komputasi ilmiah telah terbukti fleksibel dan efektif dalam berbagai bidang, termasuk pendidikan dan pemodelan matematis [18, 19]. Integrasi antara kemampuan komputasi Python, pendekatan *supervised learning*, serta teknik penyeimbangan data menghasilkan sistem deteksi yang stabil dan akurat [20]. Secara keseluruhan, temuan ini memperkuat urgensi pengembangan sistem deteksi otomatis berbasis machine learning untuk mengatasi ancaman MITM di lingkungan IIoT, yang tidak hanya berdampak pada aspek keamanan teknis, tetapi juga pada keberlanjutan operasional dan keuntungan ekonomi industri digital modern.

4. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan mengenai analisis performa algoritma machine learning dalam mendeteksi serangan Man-in-the-Middle (MitM) pada jaringan Industrial Internet of Things (IIoT), dapat ditarik beberapa kesimpulan sebagai berikut.

Pertama, algoritma berbasis pohon keputusan, yaitu *Decision Tree* dan Random Forest, menunjukkan performa yang lebih unggul dibandingkan model linier seperti *Support Vector Machine* (SVM) dalam mengklasifikasikan trafik jaringan. *Model Random Forest* mencatatkan performa terbaik dengan tingkat akurasi keseluruhan sebesar 97% hingga 98% pada berbagai skenario pengujian. Keunggulan ini juga diperkuat oleh nilai *Area Under Curve* (AUC) pada kurva ROC yang mendekati sempurna, yaitu sebesar 0,99 untuk hampir seluruh kategori serangan.

Kedua, seluruh model yang diuji memiliki kemampuan deteksi yang sangat tinggi terhadap serangan mitm_ip-spoofing, dengan nilai f1-score mencapai 1,00 pada model Decision Tree dan Random Forest. Hal ini menunjukkan bahwa fitur-fitur pada serangan manipulasi IP memiliki karakteristik yang sangat distingtif sehingga mudah dikenali oleh algoritma klasifikasi.

Ketiga, hasil penelitian menunjukkan bahwa masih terdapat tantangan dalam proses klasifikasi pada kategori serangan yang memiliki pola trafik menyerupai aktivitas normal atau benign. Serangan *mitm_arp-spoofing* dan *mitm_impersonation* merupakan kategori dengan tingkat misclassification tertinggi. Pada model SVM, tingkat *False Negative untuk arp-spoofing* mencapai 14,40%. Kondisi ini mengindikasikan adanya feature overlap antara aktivitas manipulasi jaringan dan perilaku trafik legal di lingkungan IIoT.

Keempat, penggunaan dataset dengan jumlah support yang seimbang, misalnya 67.032 atau 136.800 sampel per kelas, terbukti memberikan validitas pengujian yang kuat. Hal ini ditunjukkan oleh nilai macro average dan weighted average yang konsisten dengan nilai akurasi. Dengan demikian, model tidak menunjukkan kecenderungan bias terhadap salah satu kelas tertentu dan memiliki kemampuan generalisasi yang stabil pada data pengujian.

Kelima, untuk implementasi sistem deteksi intrusi atau *Intrusion Detection System* (IDS) yang bersifat real-time pada infrastruktur IIoT, model Random Forest direkomendasikan sebagai pilihan utama karena mampu meminimalkan False *Positive* pada trafik benign hingga 0,04%. Hal ini sangat penting untuk menjaga ketersediaan layanan jaringan agar tidak

terganggu oleh kesalahan peringatan keamanan.

Adapun keterbatasan dalam penelitian ini adalah pengujian masih dilakukan pada dataset tertentu dengan kondisi trafik yang telah terstruktur dan seimbang, sehingga belum sepenuhnya merepresentasikan kompleksitas trafik IIoT pada lingkungan nyata yang bersifat dinamis, tidak seimbang, dan berpotensi mengalami perubahan pola serangan. Selain itu, penelitian ini belum secara mendalam mengevaluasi aspek komputasi, seperti waktu pelatihan, waktu inferensi, penggunaan memori, dan efisiensi implementasi model pada perangkat IIoT dengan keterbatasan sumber daya.

Berdasarkan keterbatasan tersebut, penelitian selanjutnya disarankan untuk menguji model pada dataset IIoT yang lebih beragam dan tidak seimbang, serta melibatkan skenario serangan yang lebih kompleks dan realistis. Selain itu, penelitian lanjutan dapat mengeksplorasi metode optimasi fitur, teknik penanganan imbalance data, pendekatan deep learning, serta evaluasi performa model dari sisi efisiensi komputasi agar sistem deteksi intrusi yang dikembangkan dapat diterapkan secara lebih optimal pada lingkungan IIoT secara real-time.

Daftar Pustaka

[1] A. Widodo, T. Anissa, and I. Mubarokah, "Pemanfaatan Teknologi Industrial Internet of Things (IIoT) untuk Meningkatkan Produktivitas dan Kualitas di Industri Manufaktur", *Jurnal Pengabdian Masyarakat Bangsa*, vol. 2, no. 9, pp. 4098–4105, Nov. 2024.doi.org/10.59837/jpmba.v2i9.1623

[2] Wang, M., Sun, Y., Sun, H., & Zhang, B. (2023). *Security Issues on Industrial Internet of Things: Overview and Challenges*. *Computers, 12*(12), 256. https://doi.org/10.3390/computers12120256

[3] D. Regata Akbi and dan Ahmad Gholib Tammami, "Jurnal Politeknik Caltex Riau LIVE FORENSICS," 2021. [Online]. Available: https://jurnal.pcr.ac.id/index.php/jkt

[4] A. Irawan, W. H. N. Fadholi, Z. Erikamaretha, and F. Sinlae, "Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT," *ZTR*, vol. 6, no. 1, pp. 114–119, Apr. 2024, https://doi.org/10.36526/ztr.v6i1.3376

[5] M. A. Ali and S. A. H. Al-Sharafi, "Intrusion detection in IoT networks using machine learning and deep learning approaches for MitM attack mitigation," *Discover Internet of Things*, vol. 5, no. 1, Dec. 2025, https://doi.org/10.1007/s43926-025-00104-w.

[6] M. T. Mbejo and I. Sufian, "The Analisis Tantangan Keamanan Jaringan IoT dan Strategi Mitigasinya," *Jurnal Responsive Teknik Informatika*, vol. 9, no. 01, pp. 53–60, 2025, https://doi.org/10.36352/jr.v9i01.1178.

[7] H. Fereidouni, O. Fadeitcheva, and M. Zalai, "IoT and Man-in-the-Middle Attacks," *Security and Privacy*, vol. 8, no. 2, Mar./Apr. 2025, Art. no. e70016, https://doi.org/10.1002/spy2.7001.

[8] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, Art. no.

102419, Feb. 2020, https://doi.org/10.1016/j.jisa.2019.102419.

[9] D. Auliafitri, E. RizkiSuro, M. R. M. Malik, and A. Setiawan, "Optimalisasi Pengujian Penetrasi: Penerapan Serangan MITM (Man in the Middle Attack) menggunakan Websploit," *Journal of Internet and Software Engineering*, vol. 1, no. 3, pp. 1–12, Jun. 2024, https://doi.org/10.47134/pjise.v1i3.2620.

[10] R. A. Riadi, Y. Yuhandri, S. Sumijan, F. Pratiwi, N. Rubiati, and M. Mardayulis, "Perancangan ARP Poisioning pada Analisis Keamanan Jaringan Man In The Middle Attack pada Universitas Dumai," *Jurnal Informatika, Manajemen dan Komputer*, vol. 16, no. 1, pp. 227–235, May 2024, https://doi.org/10.36723/juri.v16i1.704.

[11] R. Rahman, A. Y. N. Leksona, and Afiqah, "Serangan Man-In-The-Middle (MITM) di Jaringan Publik: Studi dan Solusi Simulasi Serangan Password Cracking Menggunakan Hydra," *Jejak Digital: Jurnal Ilmiah Multidisiplin*, vol. 1, no. 4, pp. 2145–2156, Jul. 2025, https://doi.org/10.63822/np7skj98.

[12] A. Ba and M. Add, "Machine Learning for Intrusion Detection in IIoT: A Comprehensive Review," *Procedia Computer Science*, vol. 272, pp. 100–107, 2025, https://doi.org/10.1016/j.procs.2025.10.184.

[13] M. A. S. Arifin, A. Armanto, S. Susanto, and A. T. Martadinata, "Perbandingan Algoritma Decision Tree dan Gradient Boosting pada Model Sistem Deteksi Serangan Siber di Jaringan Internet of Things," *InComTech: Jurnal Telekomunikasi dan Komputer*, vol. 15, no. 1, pp. 41–55, Apr. 2025, https://doi.org/10.22441/incomtech.v15i1.26096.

[14] R. S. Nurhalizah, R. Ardianto, and P. Purwono, "Analisis Supervised dan Unsupervised Learning pada Machine Learning: Systematic Literature Review," *Jurnal Ilmu Komputer dan Informatika*, vol. 4, no. 1, pp. 61–72, 2024, https://doi.org/10.54082/jiki.168.

[15] R. S. Nurhalizah, R. Ardianto, and P. Purwono, "Analisis Supervised dan Unsupervised Learning pada Machine Learning: Systematic Literature Review," *Jurnal Ilmu Komputer dan Informatika*, vol. 4, no. 1, pp. 61–72, 2024, https://doi.org/10.54082/jiki.168.

[16] A. D. Ajiginni, "Identification and Classification of IP Spoofing Man in the Middle Attack on Wireless Networks Using Multilayer Perceptrons," M.Sc. thesis, School of Computing, National College of Ireland, Dublin, Ireland, 2020. [Online]. Available: https://norma.ncirl.ie/4483/

[17] W. A. Pranata and I. N. Ichsan, "Menggali Peluang Pasar dan Keuntungan Ekonomi dari Penerapan Industrial IoT," *INNOVATIVE: Journal of Social Science Research*, vol. 4, no. 6, pp. 1628–1638, Nov. 2024, https://doi.org/10.31004/innovative.v4i6.16385.

[18] N. M. Surbakti *et al.*, "Penggunaan Bahasa Pemrograman Python dalam Pembelajaran Kalkulus Fungsi Dua

Variabel," *Algoritma: Jurnal Matematika, Ilmu Pengetahuan Alam, Kebumian dan Angkasa*, vol. 2, no. 3, pp. 98–107, May 2024, https://doi.org/10.62383/algoritma.v2i3.67

[19] R. S. Nurhalizah, R. Ardianto, and P. Purwono, "Analisis Supervised dan Unsupervised Learning pada Machine Learning: Systematic Literature Review," *Jurnal Ilmu Komputer dan Informatika*, vol. 4, no. 1, pp. 61–72, 2024, https://doi.org/10.54082/jiki.168.

[20] A. Widodo, T. Anissa, and I. Mubarokah, "Pemanfaatan Teknologi Industrial Internet of Things (IIoT) untuk Meningkatkan Produktivitas dan Kualitas di Industri Manufaktur," *Jurnal Pengabdian Masyarakat Bangsa*, vol. 2, no. 9, pp. 4098–4105, Nov. 2024, https://doi.org/10.59837/jpmba.v2i9.1623