

Klasifikasi Serangan Denial of Service pada Jaringan Internet of Things Menggunakan Random Forest: Studi pada Dataset Gotham 2025

Dedet Setiawan-1^{a*}, Harma Oktavia Lingga Wijaya-2^a

^aUniversitas Bina Insan, Indonesia

Email: dedetstwn009@gmail.com^{1*}, harmaoktafialingga@gmail.com²

Abstrak

Serangan *Denial of Service* (DoS) pada jaringan *Internet of Things* (IoT) dapat mengganggu ketersediaan layanan dan komunikasi antarperangkat, sehingga diperlukan metode klasifikasi yang mampu membedakan lalu lintas normal dan lalu lintas serangan secara akurat. Penelitian ini bertujuan mengimplementasikan algoritma Random Forest untuk mengklasifikasikan serangan DoS pada jaringan IoT menggunakan dataset Gotham 2025. Penelitian dilakukan melalui eksperimen komputasional dengan dataset yang terdiri atas 2.500.000 sampel dan lima kelas, yaitu dos-http, dos-icmp, dos-syn, dos-udp, dan Normal. Data dibagi menggunakan rasio 80:20, dengan 2.000.000 sampel untuk pelatihan dan 500.000 sampel untuk pengujian. Evaluasi model dilakukan menggunakan *confusion matrix*, *classification report*, serta kurva ROC dan nilai AUC, dengan penerapan 5-fold cross-validation. Hasil pengujian menunjukkan bahwa model memperoleh akurasi sebesar 99%, dengan nilai macro F1-score dan *weighted* F1-score masing-masing sebesar 0,99. Kelas dos-http, dos-icmp, dan dos-syn memperoleh precision, recall, dan F1-score sebesar 1,00, sedangkan kelas dos-udp memiliki recall 0,99 dan kelas Normal memiliki precision 0,99. Nilai AUC untuk seluruh kelas mencapai 1,00. Hasil tersebut menunjukkan bahwa Random Forest mampu mengklasifikasikan lima kelas pada dataset dengan kinerja tinggi. Namun, pengujian pada lalu lintas jaringan nyata dan dataset eksternal masih diperlukan untuk menilai kemampuan generalisasi serta kelayakan penerapannya dalam lingkungan operasional.

Kata Kunci: *Denial of Service, Gotham 2025, Internet of Things, Klasifikasi Serangan, Random Forest*

1. Pendahuluan

Perkembangan *Internet of Things* (IoT) telah mendorong keterhubungan berbagai perangkat fisik melalui jaringan komunikasi, mulai dari perangkat rumah pintar hingga sistem pemantauan dan otomasi. Konektivitas tersebut memungkinkan pertukaran data dan pengoperasian layanan secara lebih terintegrasi, tetapi juga memperluas permukaan serangan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Sejumlah perangkat IoT memiliki keterbatasan sumber daya komputasi dan

mekanisme keamanan yang tidak selalu memadai, sehingga perlindungan jaringan menjadi tantangan penting dalam penerapan teknologi ini [1]. Kondisi tersebut menjadikan keamanan jaringan IoT sebagai persoalan teknis yang perlu ditangani melalui mekanisme pemantauan dan deteksi ancaman yang sesuai dengan karakteristik trafiknya [2].

Salah satu ancaman yang relevan pada lingkungan IoT adalah *Denial of Service* (DoS), yaitu serangan yang bertujuan mengganggu ketersediaan layanan dengan

membebani sumber daya sistem atau jaringan. Serangan DoS dapat menghasilkan trafik yang tidak wajar dan menghambat perangkat maupun layanan untuk merespons permintaan yang sah. Pada jaringan IoT, gangguan ketersediaan dapat berdampak terhadap komunikasi antar perangkat dan kelangsungan fungsi layanan yang bergantung pada pertukaran data [3]. Tantangan deteksi juga muncul karena trafik normal pada kondisi tertentu dapat memiliki volume atau pola komunikasi yang tinggi, sehingga pemisahan trafik berbahaya dan trafik normal tidak selalu dapat dilakukan hanya berdasarkan satu indikator sederhana [4].

Pendekatan keamanan jaringan tradisional umumnya memanfaatkan aturan, pola serangan yang telah diketahui, atau daftar indikator tertentu untuk mengenali aktivitas berbahaya. Pendekatan berbasis aturan dapat berguna ketika karakteristik serangan telah teridentifikasi, tetapi efektivitasnya bergantung pada ketepatan dan kemutakhiran aturan yang digunakan. Perubahan pola trafik dan kemunculan variasi serangan dapat menimbulkan kesulitan ketika aktivitas berbahaya tidak sesuai dengan pola yang telah didefinisikan sebelumnya [5]. Oleh karena itu, pembelajaran mesin (*machine learning*) menjadi salah satu pendekatan yang diteliti untuk membantu proses klasifikasi trafik jaringan berdasarkan pola yang dipelajari dari data. Model pembelajaran mesin dapat dilatih menggunakan rekaman trafik berlabel untuk mempelajari perbedaan karakteristik antara aktivitas normal dan serangan, sehingga proses deteksi tidak semata-mata bergantung pada pencocokan aturan statis [6].

Di antara algoritma pembelajaran mesin, Random Forest merupakan metode ensemble yang membangun sejumlah pohon keputusan dan menggabungkan hasil prediksinya. Metode ini telah digunakan dalam penelitian

keamanan jaringan, termasuk untuk klasifikasi trafik serangan. Penelitian mengenai pemodelan Random Forest untuk sistem deteksi intrusi jaringan menunjukkan penerapan algoritma ini pada data trafik berlabel, sementara studi lain menguji algoritma pembelajaran mesin untuk mendeteksi intrusi pada lingkungan IoT menggunakan dataset khusus IoT [7], [8]. Penelitian berbasis dataset Bot-IoT juga menunjukkan bahwa dataset tersebut dapat digunakan untuk mengevaluasi metode pembelajaran mesin dalam analisis dan identifikasi aktivitas botnet [9]. Meskipun demikian, hasil dari suatu dataset tidak secara otomatis menjamin kinerja yang sama pada dataset dengan karakteristik trafik berbeda.

Ketersediaan dataset trafik jaringan menjadi aspek penting dalam pengembangan dan evaluasi sistem deteksi intrusi. Dataset yang digunakan memengaruhi pola yang dapat dipelajari model, jenis serangan yang direpresentasikan, serta relevansi hasil evaluasi terhadap lingkungan penerapan. Penelitian terdahulu telah menggunakan dataset seperti Bot-IoT dan CICIoT2023 untuk menguji berbagai pendekatan deteksi serangan. Bot-IoT dirancang dengan menggabungkan trafik IoT yang sah dan trafik serangan yang disimulasikan, sedangkan CICIoT2023 dikembangkan sebagai dataset dan tolok ukur untuk serangan berskala besar pada lingkungan IoT [9], [10]. Penggunaan dataset tersebut memperlihatkan pentingnya data yang terstruktur untuk melatih dan mengevaluasi model deteksi intrusi.

Dataset Gotham 2025 merupakan salah satu sumber data yang dapat digunakan untuk mengkaji keamanan jaringan IoT. Dataset ini dikembangkan menggunakan Gotham testbed, yaitu lingkungan kota pintar virtual yang mencakup 78 perangkat IoT heterogen. Trafik direkam secara terdistribusi pada tingkat perangkat dan mencakup aktivitas normal serta berbagai jenis serangan,

termasuk DoS. Karakteristik ini memungkinkan analisis trafik dengan memperhatikan variasi antarperangkat dan pola komunikasi yang berbeda. Dataset tersebut memberikan sumber data untuk mengevaluasi model klasifikasi dalam lingkungan IoT virtual yang heterogen [11].

Hasil penelitian terdahulu memperlihatkan bahwa akurasi yang tinggi perlu dibaca bersama karakteristik data dan rancangan evaluasinya. Penelitian deteksi intrusi berbasis pembelajaran mesin menggunakan beragam metrik untuk menilai kemampuan model dalam membedakan aktivitas normal dan serangan, termasuk precision, recall, F-measure, serta tingkat kesalahan positif (false positive rate) [12], [13]. Metrik tersebut memberikan informasi yang berbeda misalnya, recall dapat menggambarkan proporsi sampel dari suatu kelas yang berhasil dikenali, sedangkan precision berkaitan dengan ketepatan prediksi pada kelas tersebut [14]. Oleh sebab itu, performa model perlu ditinjau dari beberapa ukuran agar keberhasilan klasifikasi secara keseluruhan tidak menutupi kesalahan pada kelas serangan tertentu.

Penelitian terdahulu juga memperlihatkan perbedaan fokus dalam pengembangan sistem deteksi. Sebagian studi menitikberatkan pada pemilihan fitur dan optimasi model, sedangkan studi lain mengembangkan pendekatan deteksi terdistribusi atau sistem yang ditujukan untuk mendukung kebutuhan operasional. Sebagai contoh, penelitian mengenai Random Forest terfederasi mengkaji penggunaan seleksi fitur untuk mendukung deteksi intrusi kolaboratif pada IoT, sementara penelitian lain menguji beberapa model pembelajaran mesin serta teknik rekayasa fitur untuk mendeteksi serangan DoS/DDoS pada jaringan IoT [15], [16]. Pendekatan tersebut menunjukkan bahwa sistem deteksi dapat dikembangkan melalui berbagai strategi, tetapi hasil dan kesimpulannya tetap berkaitan dengan

tujuan, konfigurasi, serta data eksperimen yang digunakan.

Meskipun penelitian-penelitian tersebut telah memberikan bukti penggunaan pembelajaran mesin untuk mendeteksi DoS dan DDoS, hasil dari dataset yang berbeda tidak dapat langsung dianggap mewakili kinerja model pada Dataset Gotham 2025. Bot-IoT dan CICIoT2023 memiliki rancangan serta karakteristik data masing-masing, sedangkan Gotham 2025 menyediakan rekaman trafik yang dikumpulkan pada tingkat perangkat IoT dalam lingkungan virtual heterogen [17], [18]. Dengan demikian, pengujian model pada dataset ini dapat memberikan informasi tambahan mengenai perilaku klasifikasi Random Forest dalam konteks data tersebut. Kesenjangan yang menjadi perhatian penelitian ini adalah perlunya evaluasi yang secara khusus mengkaji kinerja Random Forest untuk klasifikasi serangan DoS pada Dataset Gotham 2025, dengan tetap memperhatikan bahwa penggunaan dataset baru tidak dengan sendirinya membuktikan keunggulan model atau kesiapan penerapan di lingkungan nyata.

Penelitian ini menerapkan algoritma Random Forest untuk mengklasifikasikan trafik jaringan IoT ke dalam kategori aktivitas normal dan serangan DoS menggunakan Dataset Gotham 2025. Model dievaluasi melalui pembagian data latih dan data uji, serta pengukuran kinerja menggunakan confusion matrix, classification report, kurva *Receiver Operating Characteristic* (ROC), dan 5-fold cross-validation. Kontribusi penelitian ini adalah menyajikan evaluasi empiris penerapan Random Forest untuk klasifikasi serangan DoS pada Dataset Gotham 2025 dengan menggunakan sejumlah metrik evaluasi. Hasil penelitian diharapkan dapat menambah referensi mengenai pemanfaatan algoritma machine learning klasik dalam analisis keamanan trafik IoT serta menjadi

bahan pertimbangan bagi penelitian lanjutan yang menguji algoritma lain, membandingkan dataset, atau mengembangkan mekanisme deteksi dan mitigasi yang lebih komprehensif. Tujuan penelitian ini adalah menerapkan algoritma Random Forest untuk klasifikasi serangan DoS pada jaringan IoT menggunakan Dataset Gotham 2025 dan mengukur kinerja model berdasarkan hasil evaluasi yang dilakukan.

2. Metodologi

Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimen komputasional dengan analisis deskriptif untuk mengimplementasikan dan mengevaluasi algoritma Random Forest dalam klasifikasi serangan *Denial of Service* (DoS) pada jaringan *Internet of Things* (IoT). Pendekatan eksperimen dilakukan melalui pengolahan dataset, pembentukan model klasifikasi, pelatihan, dan pengujian menggunakan data trafik jaringan yang telah memiliki label. Analisis deskriptif digunakan untuk menjelaskan karakteristik data serta menginterpretasikan hasil evaluasi model.

Secara umum, penelitian dilaksanakan melalui beberapa tahapan, yaitu pengumpulan dataset Gotham IoT 2025, pemuatan dan pemeriksaan data, analisis distribusi kelas, pembagian data menjadi data latih dan data uji, inisialisasi algoritma Random Forest, penerapan validasi silang lima lipatan (5-fold cross-validation), pelatihan model, serta evaluasi hasil klasifikasi. Tahapan tersebut dirancang untuk mengetahui kemampuan model dalam membedakan trafik normal dan berbagai jenis serangan DoS berdasarkan karakteristik data yang tersedia.

Objek dan Sumber Data

Objek penelitian ini adalah klasifikasi trafik jaringan IoT ke dalam kategori normal dan serangan DoS menggunakan algoritma Random Forest. Data yang digunakan

merupakan data sekunder berupa dataset Gotham IoT 2025 yang diperoleh melalui repositori Zenodo. Dataset diunduh dalam format CSV dan digunakan sebagai masukan dalam proses pembentukan serta evaluasi model klasifikasi.

Dataset yang digunakan dalam proses implementasi terdiri atas 2.500.000 baris data dengan lima label kelas, yaitu dos-http, dos-icmp, dos-syn, dos-udp, dan Normal. Setiap kelas direpresentasikan oleh 500.000 data. Dengan demikian, jumlah data pada kelima kelas dalam dataset yang digunakan relatif seimbang. Label kelas berfungsi sebagai target klasifikasi yang dipelajari oleh model selama proses pelatihan.

Pengumpulan data dilakukan dengan mengunduh dataset dari sumber daring, sedangkan informasi pendukung mengenai algoritma dan proses klasifikasi diperoleh melalui studi pustaka terhadap jurnal dan literatur yang relevan. Observasi juga dilakukan untuk mengidentifikasi kebutuhan perangkat serta perangkat lunak yang digunakan dalam implementasi penelitian.

Tahapan Pengolahan Data

Pengolahan data dilakukan untuk menyiapkan dataset sebelum digunakan dalam proses pelatihan dan pengujian model. Tahapan pengolahan data dalam penelitian ini meliputi:

Pemusatan Dataset

Dataset Gotham IoT 2025 dimuat ke dalam DataFrame untuk memudahkan pengelolaan dan pemeriksaan data. Hasil pemuatan menunjukkan bahwa data yang digunakan terdiri atas 2.500.000 baris dan sembilan kolom, dengan kolom terakhir berisi label kelas.

Pemeriksaan Distribusi Kelas

Distribusi label diperiksa untuk mengetahui jumlah data pada setiap kategori. Pemeriksaan ini digunakan untuk memahami komposisi kelas sebelum model dibangun.

Pembagian Data

Dataset dibagi menjadi data latih sebesar 80% dan data uji sebesar 20%. Data latih digunakan dalam proses pembentukan model, sedangkan data uji digunakan untuk mengevaluasi kemampuan klasifikasi pada data yang tidak digunakan dalam pelatihan.

Algoritma Random Forest

Algoritma utama yang digunakan adalah Random Forest, yaitu metode supervised learning berbasis ensemble yang menggabungkan sejumlah pohon keputusan (*decision trees*) untuk menghasilkan prediksi klasifikasi. Setiap pohon dibangun menggunakan sampel data yang dipilih secara acak, sedangkan pemilihan fitur pada proses pembentukan pohon dilakukan melalui subset fitur. Untuk klasifikasi, hasil akhir ditentukan berdasarkan suara terbanyak dari pohon-pohon yang membentuk model.

Penggunaan Random Forest dalam penelitian ini ditujukan untuk mempelajari pola karakteristik trafik jaringan dan membedakan lima label kelas yang terdapat dalam dataset. Proses implementasinya meliputi inisialisasi model, pelaksanaan validasi silang, pelatihan menggunakan data latih, dan prediksi terhadap data uji.

Proses Implementasi dan Validasi Model

Implementasi model dilakukan menggunakan bahasa pemrograman Python melalui Google Colaboratory. Setelah dataset dibagi menjadi data latih dan data uji, model Random Forest diinisialisasi dan proses validasi silang lima lipatan (5-fold cross-validation) dilakukan untuk mengevaluasi model pada beberapa pembagian data. Selanjutnya, model dilatih menggunakan data latih dan digunakan untuk menghasilkan prediksi terhadap data uji.

Hasil prediksi kemudian dibandingkan dengan label aktual untuk memperoleh gambaran mengenai ketepatan klasifikasi

pada setiap kelas. Penelitian ini berfokus pada klasifikasi lima kategori, yaitu Normal, dos-http, dos-icmp, dos-syn, dan dos-udp.

Metode Evaluasi

Evaluasi kinerja model dilakukan menggunakan *confusion matrix*, *classification report*, serta kurva *Receiver Operating Characteristic* (ROC). Metrik yang digunakan meliputi *accuracy*, *precision*, *recall*, F1-score, dan *Area Under the Curve* (AUC). Metrik-metrik tersebut digunakan untuk menilai ketepatan prediksi secara keseluruhan maupun kemampuan model dalam mengenali masing-masing kelas.

Nilai *accuracy* mengukur proporsi seluruh prediksi yang benar, *precision* menunjukkan proporsi prediksi positif yang benar, sedangkan *recall* mengukur proporsi data positif aktual yang berhasil dikenali. F1-score merupakan rata-rata harmonik antara *precision* dan *recall*. Rumus yang digunakan adalah sebagai berikut:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1score = 2 \times \frac{Precision \times recall}{Precision + Recall}$$

TP (*True Positive*) adalah jumlah data positif yang diprediksi benar, TN (*True Negative*) adalah jumlah data negatif yang diprediksi benar, FP (*False Positive*) adalah jumlah data negatif yang keliru diprediksi sebagai positif, dan FN (*False Negative*) adalah jumlah data positif yang keliru diprediksi sebagai negatif. Dalam klasifikasi multikelas, nilai-nilai tersebut dihitung berdasarkan kelas yang dievaluasi.

Kurva ROC digunakan untuk menggambarkan hubungan antara *True Positive Rate* (TPR) dan *False Positive Rate*

(FPR) pada berbagai ambang keputusan, sedangkan AUC merangkum kemampuan diskriminasi model berdasarkan kurva tersebut. Evaluasi dilakukan dengan memperhatikan hasil klasifikasi setiap kelas dan nilai agregat yang ditampilkan dalam laporan klasifikasi.

3. Hasil

Karakteristik Dataset

Dataset yang digunakan dalam penelitian ini adalah Gotham IoT 2025 dalam format CSV. Data terdiri atas lima kelas, yaitu dos-http, dos-icmp, dos-syn, dos-udp, dan Normal. Setiap kelas memiliki 500.000 sampel, sehingga total dataset berjumlah 2.500.000 sampel. Distribusi data untuk setiap kelas ditampilkan pada Tabel 1.

Tabel 1. Distribusi Kelas Dataset Gotham IoT 2025

Kelas	Jumlah Sampel
dos-http	500.000
dos-icmp	500.000
dos-syn	500.000
dos-udp	500.000
Normal	500.000
Total	2.500.000

Tabel 1 memperlihatkan bahwa kelima kelas memiliki jumlah sampel yang sama. Dataset tersebut selanjutnya digunakan dalam proses pembagian data, pelatihan, dan pengujian model klasifikasi Random Forest.

Hasil Pembagian Data

Pembagian dataset dilakukan dengan proporsi 80% untuk data latih dan 20% untuk data uji. Rincian jumlah data pada masing-masing bagian disajikan pada Tabel 2.

Tabel 2. Hasil Pembagian Dataset

Jenis Data	Proporsi	Jumlah Sampel
Data Latih	80%	2.000.000
Data Uji	20%	500.000
Total	100%	2.500.000

Berdasarkan Tabel 2, sebanyak 2.000.000 sampel digunakan untuk melatih model, sedangkan 500.000 sampel digunakan

untuk menguji hasil klasifikasi. Setelah pembagian data, proses dilanjutkan dengan inialisasi model Random Forest, penerapan 5-fold cross-validation, dan pelatihan model.

Hasil Evaluasi Classification Report

Kinerja model Random Forest dievaluasi menggunakan classification report yang mencakup nilai precision, recall, dan F1-score untuk setiap kelas, serta akurasi keseluruhan. Hasil evaluasi ditampilkan pada

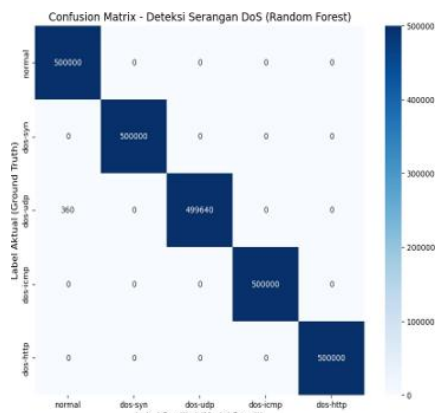
Tabel 3. Hasil Evaluasi Model Random Forest

Kelas	Precision	Recall	F1-score
dos-http	1,00	1,00	1,00
dos-icmp	1,00	1,00	1,00
dos-syn	1,00	1,00	1,00
dos-udp	1,00	1,00	1,00
Normal	0,99	1,00	0,99
Macro average (F1-score)	0,99	0,99	0,99
Weighted average (F1-score)	0,99	0,99	0,99
Akurasi keseluruhan	-	-	0,99 (99%)

Hasil pada Tabel 3 menunjukkan bahwa model memperoleh akurasi keseluruhan sebesar 99%. Kelas dos-http, dos-icmp, dan dos-syn masing-masing mencatat nilai precision, recall, dan F1-score sebesar 1,00. Kelas dos-udp memperoleh precision 1,00, recall 0,99, dan F1-score 0,99. Adapun kelas Normal memperoleh precision 0,99, recall 1,00, dan F1-score 0,99. Nilai macro average dan weighted average untuk F1-score masing-masing sebesar 0,99.

Hasil Confusion Matrix

Evaluasi menggunakan *confusion matrix* dilakukan untuk menampilkan hasil prediksi model terhadap kelas aktual.

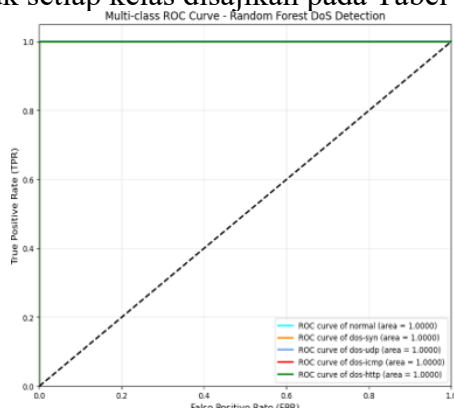


Gambar 1. Visualisasi Confusion Matrix

Visualisasi dari *confusion matrix* menyajikan jumlah prediksi benar dan salah yang dilakukan oleh model terhadap masing-masing label, dengan sumbu vertikal mewakili label sesungguhnya (*true label*) dan sumbu horizontal mewakili label prediksi (*predicted label*). Warna biru yang lebih gelap menunjukkan jumlah prediksi yang lebih tinggi, sedangkan warna lebih terang menunjukkan jumlah yang lebih rendah. Pada kelas dos-syn, dos-http, dan dos-icmp, masing-masing tercatat 500.000 prediksi benar. Sementara itu, pada kelas dos-udp, sebanyak 499.640 sampel diprediksi dengan benar dan 360 sampel diprediksi sebagai Normal.

Hasil Evaluasi Kurva ROC dan AUC

Evaluasi model juga dilakukan menggunakan kurva *Receiver Operating Characteristic* (ROC) dan nilai *Area Under the Curve* (AUC). Nilai AUC yang diperoleh untuk setiap kelas disajikan pada Tabel 5.



Gambar 2. Kurva ROC

Dari grafik terlihat bahwa semua kurva ROC dari kelima kelas berada sangat dekat dengan titik pojok kiri atas ($TPR = 1$, $FPR = 0$), yang merupakan indikasi performa klasifikasi yang sempurna. Selain itu, nilai *Area Under the Curve* (AUC) untuk seluruh kelas adalah 1.00, yang berarti model memiliki kemampuan klasifikasi yang sangat tinggi dan dapat membedakan dengan sangat baik antara masing-masing jenis serangan DoS.

Kemunculan AUC sebesar 1.00 secara konsisten untuk setiap kelas (ddos-http, ddos-icmp, ddos-syn, , ddos-udp dan data normal) menunjukkan bahwa model hampir tidak melakukan kesalahan dalam mengidentifikasi masing-masing serangan.

4. Pembahasan

Interpretasi Kinerja Model Random Forest

Hasil pengujian menunjukkan bahwa algoritma Random Forest mampu mengklasifikasikan lima kategori trafik pada dataset Gotham 2025 dengan akurasi sebesar 99%. Nilai *macro average F1-score* dan *weighted average F1-score* yang sama-sama mencapai 0,99 memperlihatkan bahwa kinerja model relatif konsisten ketika ditinjau dari rata-rata antar kelas maupun dengan mempertimbangkan jumlah sampel setiap kelas. Hasil ini menunjukkan bahwa model dapat mempelajari pola trafik yang tersedia pada dataset dan membedakan sebagian besar trafik serangan dari trafik normal. Temuan tersebut sejalan dengan penelitian sebelumnya yang menunjukkan bahwa Random Forest dapat memberikan kinerja tinggi dalam klasifikasi trafik serangan pada jaringan IoT, termasuk untuk deteksi DoS/DDoS dengan karakteristik trafik yang kompleks [19].

Kinerja tersebut perlu dipahami dalam konteks karakteristik data yang digunakan. Dataset terdiri atas lima kelas dengan jumlah sampel yang sama, yaitu masing-masing 500.000 data. Distribusi kelas yang seimbang

membuat evaluasi tidak didominasi oleh satu kelas yang jumlahnya jauh lebih besar dibandingkan kelas lain. Dengan demikian, nilai akurasi yang tinggi didukung pula oleh nilai *precision*, *recall*, dan F1-score pada masing-masing kelas, bukan hanya oleh kemampuan model mengenali kelas dengan jumlah sampel terbanyak. Kondisi distribusi kelas yang seimbang juga penting karena ketidakseimbangan data dapat menyebabkan model memberikan performa tinggi pada kelas mayoritas tetapi memiliki kemampuan deteksi yang lebih rendah pada kelas tertentu, sehingga evaluasi multi-metrik tetap diperlukan

Kinerja Klasifikasi pada Setiap Kelas

Hasil *classification report* memperlihatkan bahwa kelas dos-http, dos-icmp, dan dos-syn memperoleh nilai *precision*, *recall*, serta F1-score sebesar 1,00. Hasil tersebut menunjukkan bahwa seluruh sampel pada kelas-kelas tersebut diklasifikasikan dengan benar dalam evaluasi yang dilaporkan. Kinerja tinggi pada klasifikasi beberapa jenis serangan DoS juga telah dilaporkan pada penelitian sebelumnya yang menggunakan Random Forest untuk mendeteksi berbagai serangan berbasis IoT [21]. Meskipun demikian, hasil ini menggambarkan kinerja pada data pengujian yang digunakan dan belum dengan sendirinya membuktikan bahwa model akan memperoleh hasil identik pada trafik dari jaringan atau lingkungan yang berbeda.

Pada kelas dos-udp, model memperoleh *precision* sebesar 1,00, *recall* sebesar 0,99, dan F1-score sebesar 0,99. Perbedaan antara *precision* dan *recall* menunjukkan bahwa terdapat sebagian sampel dos-udp yang tidak berhasil dikenali sebagai dos-udp. Hal ini sejalan dengan *confusion matrix* yang mencatat 499.640 prediksi benar dan 360 sampel dos-udp yang diklasifikasikan sebagai Normal. Temuan ini menunjukkan bahwa kesalahan klasifikasi yang

teridentifikasi dalam hasil tersebut terutama berkaitan dengan sebagian kecil trafik dos-udp yang diprediksi sebagai trafik normal [22].

Sementara itu, kelas Normal memperoleh *precision* sebesar 0,99, *recall* sebesar 1,00, dan F1-score sebesar 0,99. *Recall* sebesar 1,00 menunjukkan bahwa sampel Normal pada data pengujian berhasil dikenali sebagai Normal. Namun, *precision* yang sedikit lebih rendah mengindikasikan bahwa tidak seluruh prediksi Normal berasal dari sampel yang benar-benar berlabel Normal. Oleh karena itu, penilaian terhadap kelas Normal tetap perlu mempertimbangkan *precision* dan pola kesalahan pada *confusion matrix*, selain hanya melihat nilai *recall*.

Analisis Confusion Matrix

Confusion matrix memperkuat hasil *classification report* dengan memperlihatkan jumlah prediksi benar dan kesalahan klasifikasi pada setiap kelas. Sebanyak 500.000 sampel dos-http, dos-icmp, dan dos-syn dilaporkan berhasil diklasifikasikan dengan benar. Pada kelas dos-udp, sebanyak 499.640 sampel diklasifikasikan dengan benar, sedangkan 360 sampel diprediksi sebagai Normal. Pola tersebut menunjukkan bahwa model memiliki kemampuan membedakan kelas yang tinggi pada data pengujian, tetapi masih terdapat kasus ketika trafik serangan dos-udp tidak teridentifikasi sebagai serangan.

Kesalahan antara dos-udp dan Normal menjadi aspek yang perlu diperhatikan dalam pengembangan sistem deteksi. Dalam konteks klasifikasi, kesalahan tersebut berarti sebagian trafik yang memiliki label serangan memperoleh label prediksi Normal. Apabila model digunakan sebagai bagian dari sistem pemantauan keamanan, kesalahan semacam ini dapat mengurangi kemampuan sistem untuk menandai sebagian aktivitas serangan. Oleh sebab itu, evaluasi lanjutan dapat memberi perhatian khusus pada *recall* kelas

serangan dan jenis kesalahan yang terjadi, bukan hanya pada akurasi keseluruhan. Penelitian mengenai deteksi DoS pada IoT juga menunjukkan bahwa kemampuan mendeteksi serangan perlu dianalisis berdasarkan jenis serangan dan karakteristik kesalahan, bukan hanya berdasarkan performa agregat model [23].

Analisis Kurva ROC dan Nilai AUC

Kurva ROC yang dilaporkan menunjukkan nilai AUC sebesar 1,00 untuk seluruh kelas, yaitu dos-http, dos-icmp, dos-syn, dos-udp, dan Normal. Nilai tersebut mengindikasikan kemampuan diskriminasi yang sangat tinggi berdasarkan skor prediksi yang digunakan dalam perhitungan ROC. Hasil ini melengkapi *metrik classification report* dengan sudut pandang yang berbeda, yakni kemampuan model membedakan kelas berdasarkan perubahan ambang keputusan. Evaluasi kinerja model melalui beberapa metrik diperlukan agar kemampuan klasifikasi tidak hanya dinilai berdasarkan satu ukuran performa, tetapi dapat memberikan gambaran yang lebih menyeluruh mengenai kemampuan model dalam membedakan kelas [24].

Nilai AUC sebesar 1,00 perlu dibaca bersama hasil metrik klasifikasi lainnya. Pada kelas dos-udp, misalnya, *recall* tercatat sebesar 0,99 dan *confusion matrix* menunjukkan adanya 360 kesalahan prediksi ke kelas Normal. Dengan demikian, nilai AUC yang dibulatkan menjadi 1,00 tidak seharusnya ditafsirkan sebagai bukti bahwa tidak terdapat kesalahan klasifikasi pada seluruh prediksi. AUC dan metrik berbasis hasil klasifikasi mengukur aspek kinerja yang berbeda, sehingga keduanya perlu dipertimbangkan secara bersamaan.

Implikasi dan Keterbatasan Hasil

Secara keseluruhan, hasil eksperimen menunjukkan bahwa Random Forest memberikan kinerja klasifikasi yang tinggi

pada dataset Gotham 2025 yang digunakan dalam penelitian ini. Akurasi sebesar 99%, F1-score macro dan weighted sebesar 0,99, serta nilai AUC yang dilaporkan sebesar 1,00 menunjukkan bahwa model mampu membedakan sebagian besar sampel dari lima kelas yang diuji. Temuan ini mendukung potensi penggunaan Random Forest sebagai salah satu pendekatan klasifikasi trafik untuk mendukung deteksi serangan DoS pada jaringan IoT. Penggunaan algoritma machine learning, termasuk Random Forest, telah banyak dikaji untuk menghasilkan klasifikasi dan prediksi berbasis data, tetapi penerapannya tetap perlu disesuaikan dengan karakteristik data dan tujuan penggunaannya [25].

Namun, hasil tersebut belum cukup untuk menyimpulkan bahwa model siap diterapkan secara langsung dalam lingkungan produksi atau mampu melakukan deteksi secara real-time. Pengujian yang dilaporkan berfokus pada dataset dan pembagian data yang digunakan, sehingga kemampuan generalisasi terhadap trafik dari jaringan lain belum dapat dipastikan. Selain itu, hasil yang tersedia belum memberikan pengukuran waktu inferensi, penggunaan sumber daya komputasi, maupun pengujian pada perangkat IoT dengan keterbatasan sumber daya. Aspek-aspek tersebut perlu dievaluasi lebih lanjut sebelum menarik kesimpulan mengenai efisiensi dan kelayakan penerapan operasional model.

Dengan mempertimbangkan hasil dan batasan tersebut, penelitian lanjutan dapat diarahkan pada pengujian menggunakan dataset eksternal atau trafik jaringan nyata, analisis lebih mendalam terhadap kesalahan klasifikasi dos-udp, serta pengukuran waktu pemrosesan dan kebutuhan sumber daya. Pengujian tersebut dapat memberikan gambaran yang lebih lengkap mengenai ketahanan model terhadap variasi trafik dan kelayakannya untuk mendukung sistem deteksi serangan DoS pada jaringan IoT.

5. Kesimpulan

Penelitian ini bertujuan mengimplementasikan algoritma Random Forest untuk mengklasifikasikan serangan *Denial of Service* (DoS) pada jaringan *Internet of Things* (IoT) menggunakan dataset Gotham 2025 serta mengevaluasi kinerja model dalam membedakan trafik serangan dan trafik normal. Pengujian dilakukan terhadap lima kelas, yaitu dos-http, dos-icmp, dos-syn, dos-udp, dan Normal, dengan pembagian data 80% untuk pelatihan dan 20% untuk pengujian serta penerapan 5-fold cross-validation.

Hasil evaluasi menunjukkan bahwa model memperoleh akurasi sebesar 99%, dengan macro average dan weighted average F1-score sebesar 0,99. Kelas dos-http, dos-icmp, dan dos-syn mencapai *precision*, *recall*, serta F1-score sebesar 1,00. Sementara itu, kelas dos-udp memperoleh *precision* 1,00, *recall* 0,99, dan F1-score 0,99. *Confusion matrix* menunjukkan 360 sampel dos-udp salah diklasifikasikan sebagai Normal. Nilai AUC yang dilaporkan untuk seluruh kelas adalah 1,00.

Temuan ini menunjukkan potensi Random Forest untuk mendukung klasifikasi trafik DoS pada dataset yang digunakan. Namun, hasil tersebut belum membuktikan kesiapan penerapan real-time atau kemampuan generalisasi pada jaringan berbeda. Penelitian selanjutnya disarankan menguji model pada trafik nyata atau dataset eksternal, menganalisis kesalahan klasifikasi secara lebih mendalam, serta mengevaluasi waktu inferensi dan kebutuhan sumber daya komputasi.

Daftar Pustaka

- [1] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Muñoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, 2019.
<https://doi.org/10.1016/j.comnet.2019.01.023>
- [2] Z. A. Khan and P. Herrmann, "Recent advancements in intrusion detection systems for the Internet of Things," *Security and Communication Networks*, vol. 2019, Art. no. 4301409, 2019.
<https://doi.org/10.1155/2019/4301409>
- [3] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the Internet of things: A comprehensive investigation," *Computer Networks*, vol. 160, pp. 165–191, 2019.
<https://doi.org/10.1016/j.comnet.2019.05.014>
- [4] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, Art. no. 20, 2019.
<https://doi.org/10.1186/s42400-019-0038-7>
- [5] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Applied Sciences*, vol. 9, no. 20, Art. no. 4396, 2019.
<https://doi.org/10.3390/app9204396>
- [6] A. Aljumah, "IoT-based intrusion detection system using convolution neural networks," *PeerJ Computer Science*, vol. 7, Art. no. e721, 2021.
<https://doi.org/10.7717/peerj-cs.721>
- [7] S. Farnaaz and M. A. Jabbar, "Random forest modeling for network intrusion detection system," *Procedia Computer Science*, vol. 89, pp. 213–217, 2016.
<https://doi.org/10.1016/j.procs.2016.06.047>
- [8] J. N. Sibarani, D. R. Sirait, and S. S. Ramadhanti, "Intrusion Detection Systems pada Bot-IoT Dataset menggunakan algoritma machine

- learning,” *Jurnal Masyarakat Informatika*, vol. 14, no. 1, pp. 38–52, 2023.
- [9] G. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, “Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset,” *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019. <https://doi.org/10.1016/j.future.2019.05.041>
- [10] E. C. Pinto Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, “CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment,” *Sensors*, vol. 23, no. 13, Art. no. 5941, 2023. <https://doi.org/10.3390/s23135941>
- [11] O. Belarbi, T. Spyridopoulos, E. Anthi, O. Rana, P. Carnelli, and A. Khan, “Gotham Dataset 2025: A reproducible large-scale IoT network dataset for intrusion detection and security research,” *arXiv preprint*, 2025. <https://arxiv.org/abs/2502.03134>
- [12] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, et al., “Securing Internet of Things using machine and deep learning methods: A survey,” *Cluster Computing*, vol. 27, pp. 9065–9089, 2024. <https://doi.org/10.1007/s10586-024-04509-0>
- [13] S. V. N. Santhosh Kumar, M. Selvi, and A. Kannan, “A comprehensive survey on machine learning-based intrusion detection systems for secure communication in Internet of Things,” *Computational Intelligence and Neuroscience*, vol. 2023, Art. no. 8981988, 2023. <https://doi.org/10.1155/2023/8981988>
- [14] B. R. Kikissagbe and M. Adda, “Machine learning-based intrusion detection methods in IoT systems: A comprehensive review,” *Electronics*, vol. 13, no. 18, Art. no. 3601, 2024. <https://doi.org/10.3390/electronics13183601>
- [15] A. A. Wardana, P. Sukarno, S. Basuki, dan S. B. Utomo, “Federated Random Forest with Feature Selection for Collaborative Intrusion Detection in Internet of Things,” *Procedia Computer Science*, vol. 246, hlm. 20–29, 2024. <https://doi.org/10.1016/j.procs.2024.09.193>
- [16] A. Alabdulatif, N. N. Thilakarathne, and M. Aashiq, “Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System,” *Comput. Mater. Contin.*, vol. 80, no. 3, pp. 3655–3683, 2024. <https://doi.org/10.32604/cmc.2024.054610>
- [17] M. Saied, S. Guirguis, dan M. Madbouly, “Review of artificial intelligence for enhancing intrusion detection in the Internet of Things,” *Engineering Applications of Artificial Intelligence*, vol. 127, bagian A, 2024, Art. no. 107231. Tersedia: <https://doi.org/10.1016/j.engappai.2023.107231>
- [18] J. Garcia, J. Entrena, dan A. Alesanco, “Empirical evaluation of feature selection methods for machine learning based intrusion detection in IoT scenarios,” *Internet of Things*, vol. 28, 2024, Art. no. 101367. Tersedia: <https://doi.org/10.1016/j.iot.2024.101367>
- [19] P. Elamparithi, S. Kalaivani, S. Vijayalakshmi, E. Keerthika, S. Koteswari, and R. S. Raaj, “A machine learning approach for detecting DDOS attack in IoT network using Random Forest classifier,” *International*

- Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 2s, pp. 495–502, 2023.
<https://www.ijisae.org/index.php/IJISAE/article/view/3649>
- [20] J. Li, M. S. Othman, H. Chen, and L. Mi Yusuf, “Optimizing IoT intrusion detection system: Feature selection versus feature extraction in machine learning,” *Journal of Big Data*, vol. 11, Art. no. 36, 2024.
<https://doi.org/10.1186/s40537-024-00892-y>
- [21] V. Ivanova, T. Tashev, and I. Draganov, “Random Forest detector and classifier of multiple IoT-based DDoS attacks,” *WSEAS Transactions on Information Science and Applications*, vol. 19, pp. 30–43, 2022.
<https://doi.org/10.37394/23209.2022.19.4>
- [22] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. B. Idris, S. Defit, Y. S. Triana, and R. Budiarto, “Improvement of attack detection performance on the internet of things with PSO-search and random forest,” *Journal of Computational Science*, vol. 64, Art. no. 101833, 2022.
<https://doi.org/10.1016/j.jocs.2022.101833>
- [23] E. Altulaihan, M. A. Almaiah, dan A. Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms," *Sensors*, vol. 24, no. 2, 2024, Art. no. 713. Tersedia: <https://doi.org/10.3390/s24020713>
- [24] M. Ishak, A. Wafda, and R. A. Pakkaja, “Evaluasi Sentimen Ulasan Aplikasi DeepSeek di Google Play Store menggunakan Algoritma Decision Tree,” *Journal Artificial: Informatika dan Sistem Informasi*, vol. 4, no. 1, pp. 108–122, 2026.
<https://doi.org/10.54065/artificial.1129>
- [25] A. Wafda, “Integrasi Machine Learning dalam Ritel: Tinjauan Komprehensif tentang Prediksi Harga, Analisis Data Pelanggan, dan Pemanfaatan Media Sosial,” *Journal Artificial: Informatika dan Sistem Informasi*, vol. 2, no. 2, pp. 90–106, 2024.
<https://doi.org/10.54065/artificial.543>