CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 1, Mei 2025, hlm. 34-42

Deteksi Serangan Pada Jaringan *Internet Of Things* Medis Menggunakan *Machine Learning* Dengan Algoritma *XGBoost*

Diash Firdaus[1], Afin[2], Idi Sumardi[3], Chalifa Chazar[4]

[1,2,4] Informatics, Institut Teknologi Nasional, Bandung, Indonesia
[3] Informatics Engineering, STMIK JABAR, Bandung, Indonesia

[*]Email: [1]Diash@itenas.ac.id, [2]ginz@stmikjabar.ac.id, [3]Idis@stmikjabar.ac.id, [4]chalifa@itenas.ac.id

Abstrak

Internet of Things (IoT) telah memberikan dampak besar pada sektor kesehatan, memungkinkan pengumpulan data pasien secara real-time dan meningkatkan efisiensi layanan kesehatan. Namun, adopsi perangkat IoT medis juga membawa tantangan baru terkait keamanan, terutama serangan Distributed Denial of Service (DDoS) yang dapat mengganggu layanan kritis. Penelitian ini melakukan deteksi terhadap lima jenis serangan, yaitu ARP Spoofing, Recon Attack, MQTT Attack, TCP/IP DoS, dan DDoS, menggunakan model machine learning dengan algoritma XGBoost. Dataset yang digunakan adalah CICIoMT2024, yang dirancang khusus untuk menilai keamanan perangkat medis terhubung, melibatkan 40 perangkat IoMT. XGBoost menunjukkan performa terbaik dengan akurasi, recall, presisi, dan F1-score yang unggul, mencapai akurasi 99.8%, presisi 92.4%, recall 96%, dan F1-score 93.8%. Sebelumnya, algoritma lain seperti Logistic Regression dan Naive Bayes menunjukkan akurasi masing-masing sebesar 79% dan 92% dalam mendeteksi serangan serupa, hal ini menunjukan keterbatasan dalam menangani pola yang lebih kompleks. Hasil ini menegaskan efektivitas XGBoost dalam mendeteksi ancaman keamanan dalam ekosistem IoT medis, memberikan perlindungan lebih baik terhadap potensi gangguan pada layanan kesehatan kritis.

Kata kunci: Machine Learning, Keamanan Siber, xgboost, deteksi, Internet Medical of Things

Attack Detection On Internet Medical Of Things Using Machine Learning With Xgboost Algorithm

Abstract

The Internet of Things (IoT) has significantly impacted the healthcare sector, enabling real-time patient data collection and enhancing service efficiency. However, the adoption of medical IoT devices also introduces new security challenges, particularly Distributed Denial of Service (DDoS) attacks that can disrupt critical services. This study detects five types of attacks: ARP Spoofing, Recon Attack, MQTT Attack, TCP/IP DoS, and DDoS, using machine learning models with the XGBoost algorithm. The dataset used is CICIoMT2024, specifically designed to assess the security of connected medical devices, involving 40 IoMT devices. XGBoost demonstrated the best performance with superior accuracy, recall, precision, and F1-score, achieving 99.8% accuracy, 92.4% precision, 96% recall, and 93.8% F1-score. Previously, other algorithms such as Logistic Regression and Naive Bayes showed accuracies of 79% and 92% respectively in detecting similar attacks, but with limitations in handling more complex patterns. These results underscore the effectiveness of XGBoost in detecting security threats in the medical IoT ecosystem, providing enhanced protection against potential disruptions to critical healthcare services.

Keywords*: Machine Learning, Cybersecurity,* xgboost, *detection, Internet Medical of Things*

1. PENDAHULUAN

Internet of Things (IoT) telah merevolusi berbagai sektor, termasuk sektor kesehatan. IoT medis memungkinkan pengumpulan data pasien secara real-time, pemantauan jarak jauh, dan peningkatan efisiensi layanan kesehatan (Ramadhan et al. 2024). Perangkat IoT dalam bidang kesehatan semakin banyak digunakan untuk meningkatkan kualitas layanan medis dan efisiensi operasional (Kartikasari et al. 2023). Beberapa contoh perangkat IoT di bidang kesehatan antara lain adalah monitor kesehatan berbasis IoT, seperti perangkat pemantau jantung dan tekanan darah yang dapat mengirimkan data secara real-time ke penyedia layanan kesehatan. Selain itu, terdapat perangkat wearable seperti gelang kebugaran dan jam tangan pintar yang dapat memantau aktivitas fisik, kualitas tidur, dan tanda-tanda vital lainnya. Alat bantu medis yang terhubung ke internet, seperti inhaler pintar untuk penderita asma dan pompa insulin otomatis untuk penderita diabetes, juga merupakan contoh perangkat IoT yang penting dalam manajemen penyakit kronis (Setyanto et al. 2025).

Perangkat IoT lainnya yang signifikan adalah sistem pemantauan pasien jarak jauh yang

memungkinkan dokter untuk memantau kondisi pasien di rumah sakit atau di rumah mereka sendiri (Adinda Putri et al. 2024). Contoh lainnya termasuk robot bedah yang dikendalikan dari jarak jauh untuk prosedur medis yang presisi (Humas BRIN 2023). Dalam lingkungan rumah sakit, perangkat IoT digunakan untuk manajemen inventaris dan pelacakan aset medis, seperti alat bedah dan obat-obatan, untuk memastikan ketersediaan dan efisiensi penggunaan. Adopsi perangkat IoT ini diharapkan dapat memberikan manfaat signifikan dalam meningkatkan hasil kesehatan pasien, mengurangi biaya perawatan, dan meningkatkan efisiensi operasional dalam sistem kesehatan.

Dalam menghadapi krisis kesehatan, seperti pandemi, IoT dapat berperan penting dalam memberikan pemantauan kesehatan yang lebih cepat dan respons yang tepat waktu, sehingga memerlukan sistem yang aman dan andal. Namun, dengan meningkatnya adopsi IoT dalam bidang medis, muncul pula tantangan baru terkait keamanan jaringan (Mishra and Pandya 2021). Salah satu ancaman terbesar adalah serangan Distributed Denial of Service (DDoS). Serangan DDoS adalah upaya untuk membuat layanan jaringan tidak tersedia bagi pengguna yang sah dengan membanjiri sistem dengan lalu lintas yang berlebihan (Ilman Aqilaa, Firdaus, and Naofal 2023). Dalam konteks IoT medis, serangan ini dapat menargetkan perangkat medis yang terhubung, server data, atau jaringan komunikasi (Neto et al. 2023). Serangan DDoS dapat dilakukan dengan berbagai cara, termasuk melalui botnet yang terdiri dari perangkat IoT yang telah dikompromikan. Selain itu, interoperabilitas sistem juga menjadi krusial karena perangkat IoT sering kali tidak kompatibel satu sama lain, sehingga diperlukan pengembangan standar yang memungkinkan komunikasi dan berbagi informasi yang lancar antarsistem.

Berbagai penelitian telah mengusulkan penggunaan algoritma machine learning untuk meningkatkan akurasi dan efisiensi deteksi serangan DDoS. Misalnya, *Support Vector Machines* (SVM) telah digunakan dengan sukses untuk memisahkan lalu lintas jaringan normal dan berbahaya berdasarkan fitur-fitur yang diekstraksi dengan akurasi 90% (Xie 2023). Algoritma Random Forest juga telah menunjukkan kinerja yang kuat dalam menangani dataset yang kompleks dan tidak seimbang, memberikan prediksi yang akurat dan interpretasi yang baik terhadap fitur-fitur yang relevan dalam melakukan klasifikasi serangan DDoS pada jaringan SDN (Firdaus, Munadi, and Purwanto 2020). Selain itu, logistic regression menggunakan dataset IoMT memiliki akurasi 79% (Dadkhah et al. 2024) dan Naive Bayes dengan menggunakan NF-UNSW-NB15 Dataset memiliki akurasi 92% dalam mendeteksi pola serangan DDoS dengan cepat dan efisien meskipun menghadapi keterbatasan dalam menangani data yang sangat non-linear(Samantaray, Barik, and Biswal 2024). Penelitian lain juga menyebutkan bahwa algoritma XGBoost dapat mendeteksi pola serangan DDoS dengan akurasi 98.34% akan tetapi dataset yang digunakan adalah CICDoS2019 yang bukan merupakan Dataset untuk IoT bidang Medis (Alahmadi et al. 2023).

Pada penelitian ini proses training machine learning akan menggunakan XGBoost karena memiliki akurasi yang tinggi dan menggunakan dataset IoMT (Internet of Medical Things) yang Dimana dataset ini dibuat dengan fokus dalam konteks keamanan siber di lingkungan kesehatan. Dataset CICIoMT2024 dirancang khusus untuk menilai keamanan perangkat medis yang terhubung, dengan melibatkan 40 perangkat IoMT dengan 6 jenis kelas yang berbeda, termasuk data normal, DDoS, Recon, MQTT Attack, DoS, dan spoofing (Dadkhah et al. 2024).

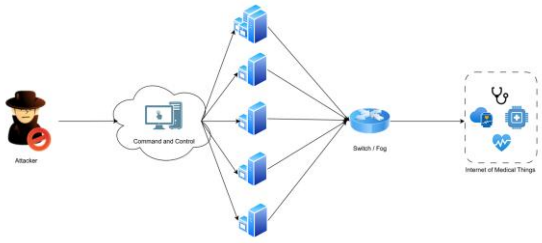
2. LANDASAN TEORI

Pada bagian ini akan dibahas landasan teori dari penelitian yang dibuat seperti pengertian dari IoMT Attack, *Machine Learning*, IoT dan *XGBoost*.

2.1. IoMT Attack

Berikut adalah jenis-jenis serangan yang dapat terjadi pada Internet of Medical Things (IoMT) :

1. DDoS *(Distributed Denial of Service)*, Serangan ini melibatkan pengiriman sejumlah besar permintaan ke perangkat atau jaringan untuk membuatnya tidak dapat diakses oleh pengguna yang sah. Dalam konteks IoMT, serangan DDoS dapat mengganggu layanan kesehatan yang kritis dengan membanjiri jaringan dengan lalu lintas yang tidak sah.
2. DoS *(Denial of Service)*, Mirip dengan DDoS, serangan DoS bertujuan untuk membuat layanan tidak tersedia dengan membanjiri target dengan permintaan yang berlebihan. Namun, DoS biasanya dilakukan dari satu sumber, berbeda dengan DDoS yang melibatkan banyak sumber.



Gambar 1. Ilustrasi Serangan DDoS

MQTT (Message Queuing Telemetry Transport) Attacks, Serangan ini menargetkan protokol komunikasi MQTT yang sering digunakan dalam perangkat IoMT. Contoh serangan termasuk MQTT

Connect Flood dan MQTT Publish Flood, yang bertujuan untuk membanjiri broker MQTT dengan permintaan koneksi atau publikasi yang berlebihan.

Spoofing, Serangan ini melibatkan pemalsuan identitas perangkat atau pengguna untuk mendapatkan akses tidak sah ke sistem. Dalam konteks IoMT, spoofing dapat digunakan untuk menyamar sebagai perangkat medis yang sah untuk mengakses data sensitif atau mengganggu operasi perangkat.

2.2. Machine Learning

Penggunaan Machine Learning (ML) dalam konteks keamanan Internet of Medical Things (IoMT) sangat penting untuk mendeteksi, mencegah, dan mengurangi serangan siber. ML dapat menganalisis pola lalu lintas jaringan dalam ruang multidimensi untuk mengidentifikasi anomali dan karakteristik serangan, seperti serangan Distributed Denial-of-Service (DDoS), Spoofing, dan sebagainya. Dengan memanfaatkan teknik ML, sistem dapat secara otomatis mendeteksi ancaman potensial, yang membantu profesional kesehatan dalam memberikan layanan berkualitas tinggi dengan pendekatan pemantauan keamanan yang berkelanjutan (Dadkhah et al. 2024).

2.3. *XGBoost*

XGBoost, atau *Extreme Gradient Boosting*, adalah algoritma pembelajaran mesin yang sangat efisien dan kuat, dirancang untuk tugas klasifikasi dan regresi. Algoritma ini dikembangkan oleh Dr. Tianqi Chen dari University of Washington pada tahun 2014 dan telah menjadi salah satu algoritma yang paling populer dan efektif dalam berbagai kompetisi dan aplikasi pembelajaran mesin12. XGBoost menggunakan teknik boosting, di mana beberapa model sederhana (biasanya decision tree) digabungkan untuk menghasilkan model yang lebih kuat. Algoritma ini memperkenalkan beberapa peningkatan signifikan dibandingkan dengan implementasi gradient boosting tradisional, termasuk regularisasi untuk mengontrol kompleksitas model dan optimasi cache-aware untuk meningkatkan efisiensi. (Fadhil 2025; Herni Yulianti, Oni Soesanto, and Yuana Sukmawaty 2022; Smadi et al. 2021).

Tahap pertama dalam proses XGBoost adalah inisialisasi, di mana nilai prediksi awal untuk seluruh data diambil dari rata-rata seluruh data.

$$L_{Split} = \frac{1}{2}\left(\frac{(\sum_{i\in I_L} g_i)^2}{\sum_{i\in I_L} h_i + \lambda} + \frac{(\sum_{i\in I_R} g_i)^2}{\sum_{i\in I_R} h_i + \lambda} - \frac{(\sum_{i\in I} g_i)^2}{\sum_{i\in I} h_i + \lambda}\right) - \gamma \qquad (1)$$

Keterangan :

F0 : Nilai rata-rata target $\bar{y}$
yi : Nilai target dari pelatihan
N : Jumlah Data

Dalam tahap inisialisasi algoritma XGBoost, model memulai dengan menetapkan prediksi awal untuk semua data sebagai rata-rata nilai target dari data pelatihan. Ini dilakukan dengan menghitung rata-rata nilai target di seluruh data pelatihan, yang kemudian digunakan sebagai prediksi awal. Prediksi awal ini menjadi dasar untuk perbaikan lebih lanjut yang akan dilakukan oleh pohon keputusan dalam iterasi selanjutnya, dengan tujuan mengurangi kesalahan prediksi secara bertahap melalui proses boosting. Setelah menetapkan prediksi awal, langkah berikutnya adalah menghitung gradient dan Hessian. Gradient adalah turunan pertama dari fungsi loss terhadap prediksi, yang menunjukkan seberapa besar kesalahan prediksi saat ini dan arah perbaikan yang diperlukan untuk model.

$$gi = \frac{\partial l(yi, \hat{y}i)}{\partial \hat{y}i} = 2(\hat{y}i - yi) \qquad (2)$$

Keterangan :

yi : Nilai actual dari data
$\hat{y}i$: adalah prediksi pada iterasi ke-i
$\hat{y}i$ $l(yi, \hat{y}i)$: Fungsi Loss
Gi : Gradient yang menunjukan seberapa besar dan arah kesalahan yang perlu dikoreksi

Tahap selanjutnya dalam proses XGBoost adalah menghitung nilai Hessian, yang merupakan turunan kedua dari fungsi kerugian terhadap prediksi. Hessian membantu mengukur kelengkungan fungsi kerugian, yang berguna untuk menentukan besarnya la36angkaherbaikan yang diperlukan.

$$hi = \frac{\partial^2 l(yi, \hat{y}i)}{\partial \hat{y}i^2} = 2 \qquad (3)$$

Keterangan
yi : Nilai actual dari data
$\hat{y}i$: adalah prediksi pada iterasi ke-i
$l(yi, \hat{y}i)$: Fungsi Loss
Hi : Hessian

Langkah berikutnya adalah memilih pembagian terbaik berdasarkan nilai Hessian dan gradient. Tahap ini bertujuan untuk menghitung pengurangan loss (atau peningkatan kualitas) setelah data dibagi menjadi dua bagian di suatu node pada pohon (split).

(4)

Keterangan
*L*split : Keuntungan (gain) dari split.
IL : Indeks dari instance yang masuk ke sisi kiri dari split.
IR : Indeks dari instance yang masuk ke sisi kanan dari split.

gi : Gradien dari fungsi loss untuk instance ke-i.
hi : Hessian, yaitu turunan kedua dari fungsi loss untuk instance ke-i.
λ : Parameter regularisasi L2 yang mengendalikan bobot pohon untuk mencegah overfitting.
γ : Minimum loss reduction yang diperlukan untuk membuat split baru dalam pohon.

.

Pada tahap ini, algoritma akan mencoba berbagai cara membagi (split) data berdasarkan fitur yang ada. Untuk setiap pembagian yang mungkin, tujuannya adalah untuk menemukan pemisahan data yang menghasilkan kelompok data yang lebih homogen, sehingga lebih dekat dengan nilai target dan dapat meningkatkan akurasi prediksi. Selanjutnya, algoritma XGBoost akan melakukan regularisasi. Regularisasi bertujuan untuk mencegah overfitting dengan menambahkan penalti terhadap kompleksitas model. Dalam konteks XGBoost, kompleksitas model diukur berdasarkan jumlah daun (leaf) pada pohon dan besar nilai pada daun tersebut.

$$\Omega(f) = \gamma T + \frac{1}{2}\lambda \sum_{j=1}^{T} w_j^2 \quad (5)$$

$\Omega(f)$: Fungsi regularisasi untuk model *f*
γ : Parameter regularisasi yang mengontrol kompleksitas model
T : Jumlah daun (leaf) pada pohon keputusan
λ : Parameter Regularisasi yang mengontrol penalty terhadap bobot daun
w_j : Bobot pada daun ke-*j*

Setelah pembangunan pohon baru, algoritma XGBoost mengevaluasi kompleksitas pohon dengan menghitung penalti yang terkait. Hal ini dilakukan untuk memastikan bahwa model tetap sederhana dan tidak terlalu mempelajari pola dari data pelatihan, yang dapat mengakibatkan overfitting. Setelah split yang optimal ditemukan dan pohon telah dibangun, langkah akhir adalah memperbarui prediksi akhir. Ini dilakukan dengan menambahkan hasil prediksi dari pohon terbaru ke prediksi sebelumnya, dengan hasil perkalian dengan learning rate η. Proses ini membantu dalam meningkatkan akurasi model secara bertahap dengan mengintegrasikan kontribusi dari setiap pohon baru yang dibangun dalam iterasi.

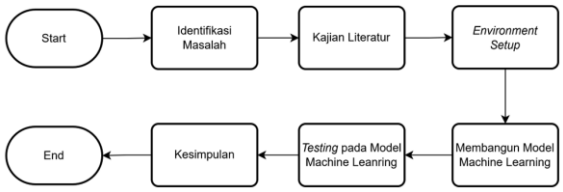
$$\hat{y}_i = \hat{y}_i + \eta\, f(x_i) \quad (6)$$

$\hat{y}i$: Nilai aktual dari data
$f(xi)$: Kontribusi pohon keputusan baru untuk input x*i*
η : Learning rate (tingkat pembelajaran)

Prediksi untuk setiap data diperbarui secara bertahap, dengan setiap pohon menambahkan koreksi kecil terhadap prediksi sebelumnya. Tujuannya adalah untuk terus mengurangi kesalahan prediksi. Learning rate digunakan untuk mengatur kecepatan pembelajaran; nilai yang lebih kecil akan memperlambat proses pembelajaran tetapi memberikan hasil yang lebih stabil, sedangkan nilai yang lebih besar akan mempercepat pembelajaran namun dapat meningkatkan risiko overfitting pada model.

3. METODE PENELITIAN

The flowchart illustrates a structured process for research or project development, delineating a sequence of steps from initiation to conclusion. Figure 1 is a flow for the research method.



Gambar 2. Alur Metode Penelitian

3.1. Identifikasi Masalah

Proses ini melibatkan pemahaman dan pendefinisian masalah yang ingin diselesaikan. Ini termasuk menentukan tujuan proyek dan mengidentifikasi kebutuhan serta tantangan yang harus diatasi.

3.2. Kajian Literatur

Tahap ini merupakan proses pemeriksaan secara komprehensif terhadap literatur yang sudah ada terkait dengan masalah yang diidentifikasi yaitu deteksi serangan DdoS menggunakan Machine Learning. Tujuannya adalah untuk mengumpulkan informasi relevan, teori, dan hasil penelitian sebelumnya yang dapat memberikan dasar untuk memahami masalah tersebut.

3.3. *Environment Setup*

Tahap ini adalah proses Mengatur *Environment* pengembangan yang diperlukan untuk penelitian, termasuk perangkat keras, perangkat lunak, dan alat yang dibutuhkan. Hal ini memastikan bahwa semua komponen teknis siap dalam mendukung pengembangan model dan melakukan test terhadap Model.

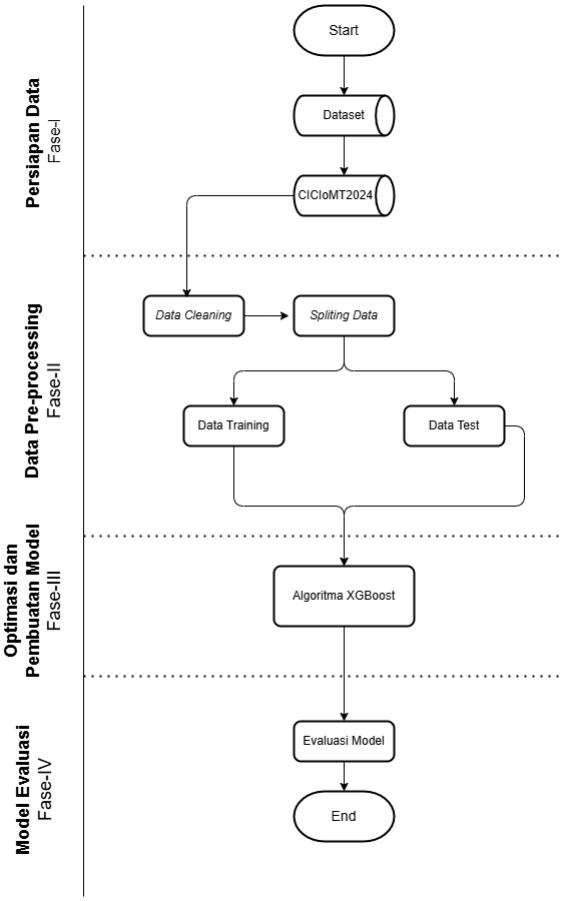
Tabel 1. Environment Setup

No	Name	Version
1	Operating System	Windows 11 Ubuntu 22
2	Client	Python
3	Server	Library Flask
4	Suppoting Tools	Raspbian for Raspberry pi
5	Hardware	CPU AMD Ryzen 7 5800

RAM 16 GB

3.4. Membangun Model *Machine Learning*

Pada tahap ini merupakan tahap pembuatan model machine learning hingga melakukan evaluasi berupa accuracy, presisi, Recall dan f1-score. Tahap ini dibagi menjadi 4 fase yaitu *Data Understanding*, *Data pre-Processing*, *Modeling* dan *Evaluation.*



Gambar 3. Alur Membangun Machine Learning Model

Fase 1 adalah Tahap Data Understanding. Tahap Data Understanding dimulai dengan persiapan dan pengumpulan data yang akan digunakan dalam proyek. Data ini disimpan dalam bentuk dataset yang menjadi dasar untuk seluruh proses analisis dan pemodelan. Dalam proyek ini, dataset yang digunakan adalah CICIoMT24, yang merupakan dataset khusus yang telah dikumpulkan dan disiapkan untuk tujuan analisis. Tahap ini penting untuk memahami karakteristik data, seperti jumlah instance, jenis fitur, dan distribusi nilai, yang akan membantu dalam merencanakan tahapan berikutnya secara efektif.

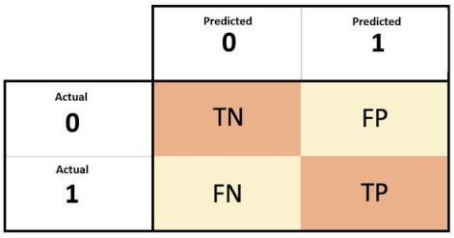
Fase 2 adalah Data Pre-Processing, dalam tahap Data Pre-processing, data yang dikumpulkan diolah untuk persiapan pemodelan. Proses ini dimulai dengan data cleaning, yang melibatkan membersihkan data dari kesalahan, nilai yang hilang, atau anomali yang dapat mempengaruhi hasil analisis. Setelah itu, skala fitur data di standarisasi menggunakan Standar Scaler untuk memastikan bahwa semua fitur memiliki kontribusi yang sama dalam pemodelan. Data yang telah di-clean dan di-scale kemudian dikonversi menjadi format DMatrix yang sesuai untuk digunakan dalam algoritma XGBoost. Terakhir, data dibagi menjadi dua subset: data training dan data testing. Data training digunakan untuk melatih model, sementara data testing digunakan untuk menguji performa model.

Fase 3 adalah Tahap Optimasi dan Pembuatan model dimana pada fase ini melibatkan pembangunan model dan optimasi model menggunakan algoritma XGBoost. Subset data training digunakan untuk melatih model, dimana model belajar dari pola dan hubungan dalam data. Setelah itu, subset data testing digunakan untuk mengevaluasi kinerja model yang telah dilatih, memastikan bahwa model dapat memprediksi dengan akurat pada data yang belum pernah dilihat sebelumnya. Pemodelan dilakukan menggunakan algoritma XGBoost, yang merupakan metode gradient boosting yang kuat untuk masalah klasifikasi dan regresi. Tahap ini juga melibatkan optimasi hyperparameter untuk meningkatkan kinerja model.

Fase 4 adalah Tahap Evaluation. Tahap Evaluation adalah tahap terakhir dalam proses ini, dimana model yang telah dibangun dan dioptimalkan diuji dalam lingkungan yang sesungguhnya untuk memastikan kinerja dan keandalannya dalam kondisi nyata. Kinerja model dievaluasi berdasarkan metrik seperti akurasi, presisi, recall, dan F1-score untuk memastikan bahwa model memenuhi standar yang diharapkan. Hasil evaluasi dan kesimpulan dari pemodelan dikumpulkan dan dilaporkan, menandai penyelesaian proses. Tahap ini penting untuk memvalidasi keefektivitan model dan memastikan bahwa model siap untuk digunakan dalam aplikasi praktis.

3.5. *Testing* dan *Performance Evaluation Metrics*

Evaluasi model dilakukan untuk mengukur sejauh mana kemampuan model dalam melakukan deteksi. Proses evaluasi ini melibatkan pengukuran nilai error dalam deteksi melalui beberapa metode, termasuk Classification Report dan Confusion Matrix. Untuk menguji kinerja klasifikasi algoritma yang dibangun. (Fathan Hidayatullah & Sn, 2014; Hastuti, 2012). Perhitungan nilai Akurasi, presisi, recall, dan F1-Score merupakan langkah penting dalam penilaian kinerja algoritma untuk menentukan tingkat keakuratan model. Hasil perhitungan ini ditampilkan dalam Gambar 2 berikut.



Gambar 4 *Confussion Matrix* (Firdaus and Rianti 2023)

True Positive (TP) adalah prediksi yang benar-benar positif, di mana nilai prediksi dan nilai sebenarnya keduanya positif. True Negative (TN) adalah prediksi yang benar-benar negatif, di mana nilai prediksi dan nilai sebenarnya keduanya negatif. False Positive (FP) terjadi ketika prediksi positif, tetapi nilai sebenarnya adalah negatif. False Negative (FN) adalah prediksi negatif, padahal nilai sebenarnya adalah positif (Fadhil 2025). Rumus untuk evaluasi klasifikasi dapat dilihat pada Persamaan (7), (8), (9) dan (10) berikut.

$$\text{Akurasi} = \frac{TP+TN}{TP+TN+FP+FN} \quad (7)$$

$$\text{Presisi} = \frac{TP}{TP+FP} \quad (8)$$

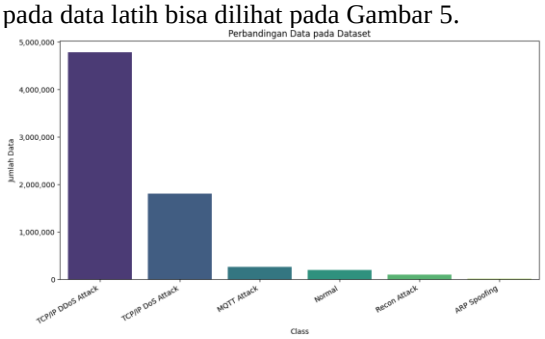
$$\text{Recall} = \frac{TP}{TP+FN} \quad (9)$$

$$F1\text{-Score} = \frac{2\times(\text{Presisi}\times\text{Recall})}{\text{Presisi}+\text{Recall}} \quad (10)$$

4. HASIL DAN DISKUSI

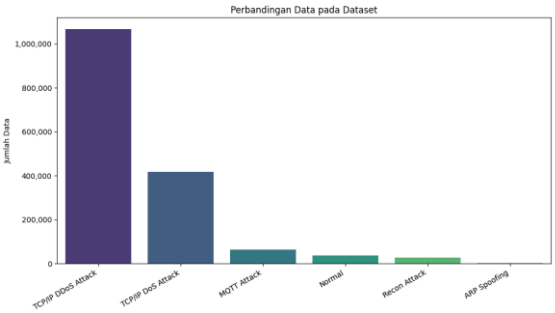
Pada penelitian ini, dataset yang digunakan adalah CICIoMT2024. CICIoMT2024 adalah sebuah dataset benchmark yang dirancang untuk penilaian keamanan multi-protokol dalam Internet of Medical Things (IoMT). Dataset ini dikembangkan untuk mengatasi kekurangan pada dataset benchmark yang ada, seperti jumlah perangkat nyata yang terbatas, variasi serangan yang kurang, dan kurangnya profil yang luas. CICIoMT2024 mencakup 18 serangan yang dieksekusi pada testbed IoMT dengan 40 perangkat, yang terdiri dari 25 perangkat nyata dan 15 perangkat simulasi, menggunakan protokol seperti Wi-Fi, MQTT, dan Bluetooth (Dadkhah et al. 2024). Sebagai perbandingan, CICDDoS2019 (Sharafaldin et al. 2019) adalah dataset yang lebih umum digunakan untuk mendeteksi intrusi jaringan dan mencakup berbagai jenis serangan siber seperti DoS, DDoS, dan serangan lainnya, tetapi tidak secara khusus berfokus pada perangkat IoMT atau protokol yang digunakan dalam konteks medis17. KDDCup (Yang and Zhao 2019) adalah dataset yang lebih tua dan sering digunakan sebagai benchmark dalam penelitian deteksi intrusi, tetapi juga tidak memiliki fokus khusus pada IoMT atau protokol medis.

Jumlah perbandingan Data Serangan dan Normal pada data latih bisa dilihat pada Gambar 5.



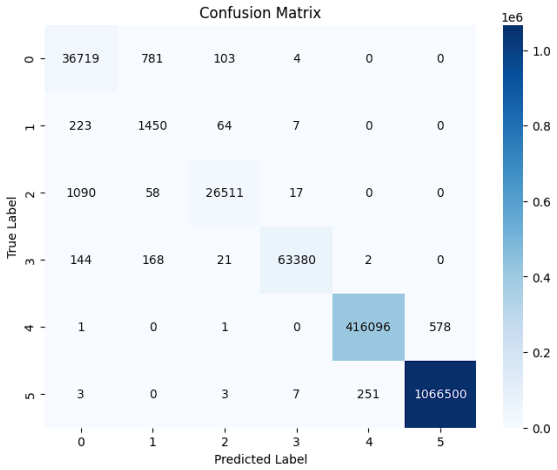
Gambar 5. Perbandingan kelas pada data latih

sedangkan jumlah perbandingan Data Serangan dan normal pada data Test bisa dilihat pada Gambar 6.



Gambar 6. Perbandingan kelas pada data uji

tahap berikutnya adalah proses standar scaler, proses standar scaler adalah memastikan bahwa semua fitur memiliki kontribusi yang sama dalam pemodelan. Setelah selesai Data yang telah di-clean dan di-scale kemudian dikonversi menjadi format DMatrix yang sesuai untuk digunakan dalam algoritma XGBoost. Setelah semua selesai maka proses berikutnya adalah traing model menggunakan Dataset. Hasil dari Training dan testing model dievaluasi menggunakan confusin matrix yang bisa dilihat pada gambar blablabla.



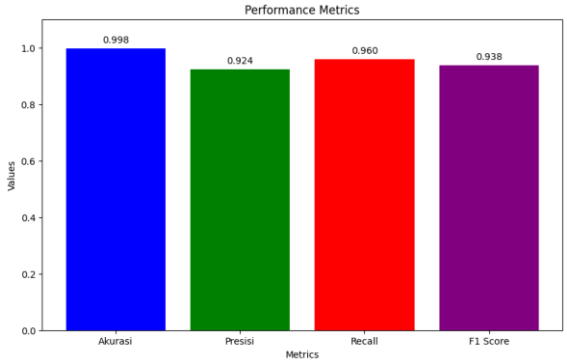
Gambar 7. hasil dari Confusion Matrix Model

Confusion matrix ini menggambarkan kinerja model klasifikasi yang bekerja pada enam kelas yang berbeda. Setiap baris menunjukkan label sebenarnya, sedangkan setiap kolom mewakili label yang diprediksi oleh model. Diagonal utama dari matriks ini menunjukkan jumlah sampel yang diklasifikasikan dengan benar, yang dikenal sebagai true positives. Misalnya, model ini berhasil mengklasifikasikan 36.719 sampel dengan label sebenarnya 0 sebagai 0, dan 1.066.500 sampel dengan label sebenarnya 5 juga diklasifikasikan dengan benar sebagai 5, menunjukkan kinerja yang baik untuk kelas-kelas ini.

Di sisi lain, angka di luar diagonal menunjukkan kesalahan klasifikasi. Sebagai contoh, ada 781 sampel yang seharusnya diklasifikasikan sebagai 0 tetapi diprediksi sebagai 1, dan 1.090 sampel dengan label sebenarnya 2 yang diklasifikasikan sebagai 0. Ini menunjukkan bahwa ada beberapa kebingungan antara kelas-kelas tertentu.

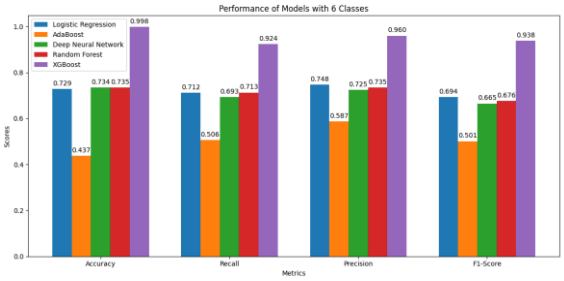
Secara keseluruhan, model ini menunjukkan kinerja yang kuat pada kelas dengan angka tinggi di diagonal, seperti kelas 5. Namun, ada ruang untuk perbaikan, terutama dalam mengurangi jumlah kesalahan klasifikasi pada kelas lain. Selain itu, perbedaan besar dalam jumlah sampel yang diklasifikasikan dengan benar menunjukkan adanya kemungkinan ketidakseimbangan dalam dataset, di mana beberapa kelas mungkin memiliki lebih banyak sampel daripada yang lain, mempengaruhi performa model secara keseluruhan.

Berdasarkan hasil dari training dan testing menggunakan algoritma XGBoost, hasil yang daidapatkan adalah nilai akurasi sebesar 99.8 %. Kemudian presisi 92.4%, Recall 96%, F1-Score sebesar 93.8% hasil ini bisa dilihat juga pada Gambar blablabla.



Gambar 8. Hasil Akurasi, Presisi, Recall dan F1-Score

Selanjutnya, hasil dari evaluasi model yang telah dibuat dibandingkan dengan model lain dari penelitian sebelumnya yang dibuat oleh (Dadkhah et al. 2024). Hasil akurasi, presisi, recall dan f1 score yang dihasilkan model machine learning menggunakan Xgboost pada dataset CICIoMT2024 memiliki keakuratan yang lebih unggul dibandingkan dengan model Logistic Regression, Adaboost, DNN dan Random Forest khususnya pada model dengan 6 kelas. Gambar blablabla merupakan perbandingan dari model XGboost dan model lainyya.



Gambar 9. Perbandingan Akurasi, Presisi, Recall dan F1-score XGBoost dengan algoritma lain

Grafik ini menggambarkan kinerja lima teknik machine learning dalam mengklasifikasikan data menjadi enam kelas, diukur melalui empat metrik: akurasi, recall, presisi, dan F1-score. Model yang diuji meliputi Logistic Regression, AdaBoost, Deep Neural Network, Random Forest, dan XGBoost. XGBoost menonjol sebagai model dengan performa terbaik, menunjukkan skor tertinggi pada semua metrik: akurasi mencapai 0.998, recall 0.924, presisi 0.960, dan F1-score 0.938. Random Forest dan Deep Neural Network juga menunjukkan kinerja yang baik, khususnya pada metrik presisi dan akurasi, dengan nilai presisi dan akurasi masing-masing sekitar 0.735 dan 0.734 untuk Deep Neural Network.

Sementara itu, Logistic Regression menunjukkan performa yang solid dengan nilai akurasi 0.729 dan presisi 0.748, meskipun sedikit lebih rendah dibandingkan XGBoost. Sebaliknya, AdaBoost tampil kurang optimal dibandingkan model lain di semua metrik, dengan nilai terendah pada recall (0.506) dan F1-score (0.501).

Secara keseluruhan, grafik pad Gambar 9. mengilustrasikan bahwa XGBoost secara konsisten mengungguli model lain dalam konteks klasifikasi multi-kelas, diikuti oleh Random Forest dan Deep Neural Network yang juga menawarkan kinerja kompetitif. XGBoost lebih unggul dalam klasifikasi multi-kelas karena beberapa alasan sederhana. Model ini secara cerdas menggabungkan banyak pohon keputusan kecil untuk memperbaiki kesalahan sebelumnya, sehingga lebih akurat dan presisi.

5. KESIMPULAN

Kesimpulan dari penelitian ini adalah model Machine learning dengan algoritma XGBoost dapat melakukan klasifikasi multi-kelas yang baik dibandingkan dengan model lain, yaitu Logistic Regression, AdaBoost, Deep Neural Network, dan Random Forest. Berdasarkan analisis terhadap empat metrik kinerja—akurasi, recall, presisi, dan F1-score—XGBoost menunjukkan performa terbaik dengan skor tertinggi di semua metrik: akurasi mencapai 0.998, recall 0.924, presisi 0.960, dan F1-score 0.938, menjadikannya pilihan utama untuk

deteksi serangan DDoS yang membutuhkan tingkat akurasi dan presisi tinggi khususnya pada bidang klasifikasi serangan DDoS pada IoMT. Keunggulan XGBoost terutama disebabkan oleh kemampuannya menggabungkan banyak pohon keputusan kecil untuk memperbaiki kesalahan sebelumnya, sehingga meningkatkan akurasi secara keseluruhan.

Kami berharap Dalam menghadapi ketidakseimbangan kelas dalam dataset CICIoMT2024, penting untuk menerapkan strategi yang efektif guna memastikan model dapat mendeteksi semua kelas dengan akurasi yang memadai. Salah satu pendekatan yang dapat diambil adalah resampling data, baik melalui oversampling kelas minoritas untuk menambah jumlah sampel atau undersampling kelas mayoritas untuk mengurangi dominasi mereka. Selain itu, penggunaan algoritma khusus seperti SMOTE (Synthetic Minority Over-sampling Technique) dapat membantu menciptakan sampel sintetis untuk kelas yang kurang terwakili.

DAFTAR PUSTAKA

Adinda Putri, Risa, Yesha Daniela Aedo, Indra Wijaya, Muhammad Roihan Jannatun Adhen, and Dicky Pratama. 2024. "JURNAL REIN (REKAYASA INFORMATIKA) Analisis Implementasi Internet Of Thing Dalam Bidang Kesehatan: Systematic Literature Review." 1(1):66–72.

Alahmadi, Amal A., Malak Aljabri, Fahd Alhaidari, Danyah J. Alharthi, Ghadi E. Rayani, Leena A. Marghalani, Ohoud B. Alotaibi, and Shurooq A. Bajandouh. 2023. "DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions." *Electronics (Switzerland)* 12(14):1–24. doi: 10.3390/electronics12143103.

Dadkhah, Sajjad, Euclides Carlos Pinto Neto, Raphael Ferreira, Reginald Chukwuka Molokwu, Somayeh Sadeghi, and Ali A. Ghorbani. 2024. "CICIoMT2024: A Benchmark Dataset for Multi-Protocol Security Assessment in IoMT." *Internet of Things (Netherlands)* 28(July). doi: 10.1016/j.iot.2024.101351.

Fadhil, Nazwa. 2025. "Perbandingan Akurasi Algoritma Xgboost Dan Svr Dalam Prediksi Harga Cryptocurrency." *JIKSI (Jurnal Ilmu Komputer Dan Sistem Informasi)* 13(1):1–4.

Firdaus, Diash, Rendy Munadi, and Yudha Purwanto. 2020. "DDoS Attack Detection in Software Defined Network Using Ensemble K-Means++ and Random Forest." *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2020* 164–69. doi: 10.1109/ISRITI51436.2020.9315521.

Firdaus, Diash, and Resa Rianti. 2023. "DETEKSI ANOMALI DAN SERANGAN LOW RATE DDOS DALAM LALU LINTAS JARINGAN MENGGUNAKAN NAIVE BAYES." 05(02):140–48.

Herni Yulianti, Sri Elina, Oni Soesanto, and Yuana Sukmawaty. 2022. "Penerapan Metode Extreme Gradient Boosting (XGBOOST) Pada Klasifikasi Nasabah Kartu Kredit." *Journal of Mathematics: Theory and Applications* 4(1):21–26. doi: 10.31605/jomta.v4i1.1792.

Humas BRIN. 2023. "BRIN - Telesurgery, Operasi Bedah Jarak Jauh Dengan Robot Bedah." Retrieved February 5, 2025 (https://brin.go.id/news/116216/telesurgery-operasi-bedah-jarak-jauh-dengan-robot-bedah).

Ilman Aqilaa, Muhammad, Diash Firdaus, and Nawaf Naofal. 2023. "Identifikasi Serangan Lowrate Distributed Denial Of Services Dalam Jaringan Dengan Menggunakan Algoritma Adaboost." *Simpatik: Jurnal Sistem Informasi Dan Informatika* 3(1):34–41. doi: 10.31294/simpatik.v3i1.1829.

Kartikasari, Diah Putri, Tengku Syahvina, Rival Dini, Puji Sri Alhirani, Pebi Mina Husania, Tiara Ayu, Triarta Tambak, and Program Studi. 2023. "Pengaruh Internet of Things (IoT) Dalam Bidang Kesehatan Terhadap Masyarakat Umum." *IJESPG (International Journal of Engineering, Economic, Social Politic and Government)* 1(3):21–26.

Kotey, Seth Djane, Eric Tutu Tchao, and James Dzisi Gadze. 2019. "On Distributed Denial of Service Current Defense Schemes." *Technologies* 7(1). doi: 10.3390/technologies7010019.

Mishra, Nivedita, and Sharnil Pandya. 2021. "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review." *IEEE Access* 9:59353–77. doi: 10.1109/ACCESS.2021.3073408.

Neto, Euclides Carlos Pinto, Sajjad Dadkhah, Raphael Ferreira, Alireza Zohourian, Rongxing Lu, and Ali A. Ghorbani. 2023. "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment." *Sensors* 23(13):5941. doi: 10.3390/s23135941.

Ramadhan, Irfan Wahyu, Sisdarmanto Adinandra, Program Studi, Magister Teknik, Rekayasa Elektro, Fakultas Teknik Industri, Universitas Islam Indonesia, and Kecerdasan Buatan. 2024. "Penerapan IoT Dalam Sistem Monitoring Kesehatan : Inovasi Dan Implementasi." 23(4):763–72.

Samantaray, Milan, Ram Chandra Barik, and Anil Kumar Biswal. 2024. "A Comparative Assessment of Machine Learning Algorithms

in the IoT-Based Network Intrusion Detection Systems." *Decision Analytics Journal* 11(December 2023). doi: 10.1016/j.dajour.2024.100478.

Setyanto, Dhoni, Puji Laksmini, Universitas Garut, Fakultas Ilmu Kesehatan, and Universitas Siliwangi. 2025. "Studi Literatur Penggunaan Internet of Things (IoT) Dalam Sektor Kesehatan." 26–37.

Sharafaldin, Iman, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani. 2019. "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy." *IEEE 53rd International Carnahan Conference on Security Technology*.

Smadi, Sami, Omar Almomani, Adel Mohammad, Mohammad Alauthman, and Adeeb Saaidah. 2021. "VPN Encrypted Traffic Classification Using XGBoost." *International Journal of Emerging Trends in Engineering Research* 9(7):960–66. doi: 10.30534/ijeter/2021/20972021.

Wani, Sharyar, Mohammed Imthiyas, Hamad Almohamedh, Khalid M. Alhamed, Sultan Almotairi, and Yonis Gulzar. 2021. "Distributed Denial of Service (Ddos) Mitigation Using Blockchain—a Comprehensive Insight." *Symmetry* 13(2):1–21. doi: 10.3390/sym13020227.

Xie, Yafei. 2023. "Machine Learning-Based DDoS Detection for IoT Networks." *Applied and Computational Engineering* 29(1):99–107. doi: 10.54254/2755-2721/29/20230972.

Yang, Lingfeng, and Hui Zhao. 2019. "DDoS Attack Identification and Defense Using SDN Based on Machine Learning Method." *Proceedings - 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2018* 174–78. doi: 10.1109/I-SPAN.2018.00036.