InComTech: Jurnal Telekomunikasi dan Komputer
vol.16, no.1, April 2026, 43-57
http://publikasi.mercubuana.ac.id/index.php/Incomtech
P-ISSN: 2085-4811 E-ISSN: 2579-6089

Deteksi Serangan Siber pada Perangkat Kesehatan Berbasis WiFi dan MQTT dengan Machine Learning

Roymond Chandra Pradana[1*], Alva Hendi Muhammad [2]

[1] *Program Studi S2 PJJ Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta, Jl. Ring Road Utara, Condong Catur, Sleman, Yogyakarta, Indonesia*

*Email Penulis Koresponden: roymond.chandra93@students.amikom.ac.id

Abstrak **:**
Penelitian ini membahas deteksi serangan siber pada Internet of Medical Things (IoMT) berbasis protokol WiFi dan MQTT menggunakan model machine learning. IoMT semakin rentan terhadap serangan seperti DoS, spoofing, dan reconnaissance yang mengancam ketersediaan dan kerahasiaan data medis. Dengan memanfaatkan dataset CICIoMT2024, tujuh algoritma diuji, yaitu Random Forest, XGBoost, CatBoost, LightGBM, SVM, KNN, dan SGD Classifier. Evaluasi dilakukan terhadap tiga skenario klasifikasi (dua, enam, dan 19 kategori) menggunakan metrik akurasi, precision, recall, dan f1-score untuk menilai sensitivitas model terhadap variasi serangan. Hasil pengujian menunjukkan bahwa algoritma ensemble, khususnya Random Forest, memberikan performa terbaik dengan akurasi 99,85% dan f1-score 0,9838. Model ini juga lebih stabil dalam mendeteksi serangan minoritas seperti MQTT-DoS dan Recon. Temuan ini menunjukkan bahwa pendekatan ensemble efektif untuk memperkuat sistem deteksi intrusi IoMT lintas protokol secara lebih akurat dan adaptif pada lingkungan medis modern.

Kata Kunci:
serangan siber***;***
machine learning;
Internet of Medical Things***;***
deteksi serangan

Riwayat Artikel:
Diserahkan 05 November 2025
Direvisi 26 November 2025
Diterima 22 Februari 2026

DOI:
10.22441/incomtech.v16i1.32219

1. PENDAHULUAN

Perkembangan teknologi Internet of Medical Things (IoMT) telah membawa transformasi besar dalam sistem layanan kesehatan modern. Melalui perangkat medis cerdas yang mampu memantau kondisi pasien secara real-time, IoMT memberikan efisiensi dan akurasi tinggi dalam pengumpulan serta pertukaran data medis. Integrasi dengan protokol komunikasi nirkabel seperti WiFi dan Message Queuing Telemetry Transport (MQTT) memungkinkan proses transmisi data yang

cepat, efisien, dan berkelanjutan antar perangkat medis maupun sistem rumah sakit. Namun, keterhubungan ini juga menghadirkan risiko keamanan yang signifikan. Serangan siber terhadap perangkat IoMT dapat menyebabkan gangguan layanan, kebocoran data pasien, bahkan membahayakan keselamatan pasien jika perangkat medis dikompromikan. Laporan Badan Siber dan Sandi Negara (BSSN, 2024) mencatat lebih dari 80.000 anomali lalu lintas jaringan pada perangkat IoT di Indonesia, menunjukkan bahwa ancaman terhadap infrastruktur IoMT semakin meningkat dan kompleks.

Berbagai penelitian telah dilakukan untuk mendeteksi dan mengurangi risiko serangan siber pada IoMT. Penelitian Hindy et al. menunjukkan efektivitas algoritma machine learning dalam mendeteksi serangan berbasis MQTT dengan akurasi mencapai 97%[1]. Khan et al. (2021) memanfaatkan pendekatan *deep learning* dan mencatat akurasi 99,92% untuk klasifikasi biner [2]. Gorzalczany dan Rudzinski (2022) menggabungkan logika *fuzzy* dengan pembelajaran mesin untuk meningkatkan interpretabilitas hasil deteksi [3], sementara Siddharthan et al. (2022) mengusulkan metode *ensemble multi-cascade* yang mencapai akurasi di atas 99% [4]. Dalam konteks protokol WiFi, Thamilarasu et al. (2020) dan Vaccari et al. (2021) menegaskan bahwa WiFi sering kali dikonfigurasi dengan sistem keamanan yang lemah, membuatnya rentan terhadap serangan *Denial of Service (DoS)* dan *Man-in-the-Middle (MiTM)* yang berpotensi digunakan untuk eksfiltrasi data medis[5], [6]. Alsolami et al. mengevaluasi berbagai model ensemble learning dalam mendeteksi serangan pada IoMT healthcare dan melaporkan kinerja yang lebih baik dibandingkan metode tunggal [7]. Ibrahim dan Al-Wadi menekankan pentingnya penggabungan beberapa algoritma berbasis ensemble untuk memperkuat keamanan IoMT dengan akurasi yang sangat tinggi [8].

Selain itu, penelitian oleh Alalhareth dan Hong [9] memperkenalkan pendekatan meta-learning dengan ensemble IDS yang terbukti meningkatkan performa deteksi secara adaptif pada skenario IoMT. Penelitian terbaru oleh Ariana et al. (2024) mengembangkan sistem deteksi intrusi menggunakan ensemble learning pada IoT dengan hasil akurasi tinggi, memperkuat bukti bahwa algoritma ensemble unggul dalam konteks protokol serangan yang kompleks [10].Alani et al. menekankan pentingnya metode *ensemble explainable* untuk meningkatkan akurasi dan interpretabilitas sistem deteksi serangan di IoMT [11]. Penelitian terbaru Dadkhah et al. memperkenalkan dataset CICIoMT2024, yang menyediakan benchmark multi-protokol termasuk MQTT dan WiFi, namun masih terbatas pada beberapa algoritma klasik [12]. Selain itu, penelitian oleh Kulshrestha dan Vijay Kumar **(2023)** mengembangkan sistem deteksi intrusi berbasis *machine learning* untuk lingkungan IoMT dengan memanfaatkan algoritma *Random Forest*, *Gradient Boosting*, dan *Support Vector Machine*. Hasilnya menunjukkan bahwa pendekatan berbasis *ensemble learning* mampu meningkatkan akurasi serta stabilitas deteksi pada dataset IoMT yang kompleks[13].

Meskipun hasil penelitian terdahulu cukup menjanjikan, sebagian besar masih terbatas pada skenario klasifikasi sederhana (dua atau enam kelas) dan berfokus pada satu protokol komunikasi saja, seperti MQTT. Selain itu, pendekatan yang digunakan umumnya berbasis model tunggal (single learner) dan belum

memanfaatkan secara optimal algoritma ensemble modern seperti *Random Forest*, *XGBoost*, *CatBoost*, dan *LightGBM* yang terbukti memiliki kemampuan lebih baik dalam menangani pola serangan yang kompleks dan tidak linear. Dataset terbaru CICIoMT2024 yang mencakup 19 kategori serangan lintas protokol WiFi dan MQTT juga belum banyak dimanfaatkan dalam penelitian komparatif secara komprehensif, sehingga celah ini membuka peluang untuk penelitian lanjutan yang lebih mendalam dan realistis terhadap kondisi jaringan IoMT sebenarnya.

Berdasarkan kondisi tersebut, penelitian ini berangkat dari permasalahan utama bahwa belum ada model deteksi serangan yang mampu mengidentifikasi berbagai jenis serangan pada IoMT secara efektif dengan mempertimbangkan variasi protokol dan kompleksitas data multi-kelas. Selain itu, sebagian model yang ada masih memiliki kelemahan dalam mendeteksi kelas serangan minoritas (minor attacks) seperti *spoofing* dan *reconnaissance*, yang walaupun jarang terjadi, berpotensi menjadi tahap awal dari serangan yang lebih besar. Oleh karena itu, diperlukan pendekatan yang tidak hanya berfokus pada peningkatan akurasi, tetapi juga sensitif terhadap variasi dan dampak serangan terhadap ekosistem IoMT.

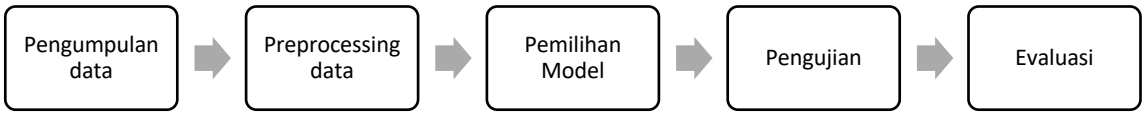
Untuk menjawab tantangan tersebut, penelitian ini menggunakan pendekatan machine learning ensemble yang telah terbukti unggul dalam meningkatkan performa deteksi pada sistem keamanan jaringan. Tujuh algoritma pembelajaran mesin modern diuji dan dibandingkan, yaitu Random Forest, XGBoost, CatBoost, LightGBM, SVM, KNN, dan SGD Classifier, dengan menggunakan dataset CICIoMT2024. Evaluasi dilakukan berdasarkan empat metrik utama, yaitu akurasi, precision, recall, dan F1-score, pada tiga skenario klasifikasi yang berbeda: dua kategori (normal dan serangan), enam kategori, dan sembilan belas kategori. Pendekatan ini memungkinkan analisis yang lebih luas terhadap kemampuan tiap model dalam mendeteksi variasi serangan, termasuk serangan multi-protokol yang kompleks.

Penelitian ini berkontribusi dalam tiga aspek utama. Pertama, menghadirkan analisis komparatif terbaru terhadap tujuh algoritma machine learning modern pada dataset multi-protokol CICIoMT2024, yang belum banyak dilakukan pada penelitian sebelumnya. Kedua, hasil penelitian ini mengidentifikasi bahwa algoritma ensemble, khususnya Random Forest, memberikan performa paling stabil dengan akurasi hingga 99,85% dan F1-score 0,9838, serta mampu mengenali serangan minor dengan tingkat kesalahan rendah. Ketiga, penelitian ini memberikan kontribusi praktis berupa rekomendasi penerapan arsitektur hybrid intrusion detection system (IDS), di mana model ringan diterapkan di perangkat ujung (*edge devices*) untuk deteksi cepat, sedangkan model ensemble dengan akurasi tinggi digunakan di server pusat untuk analisis mendalam.

Dengan pendekatan tersebut, penelitian ini tidak hanya memberikan peningkatan akurasi deteksi secara signifikan, tetapi juga memperkuat ketahanan sistem keamanan IoMT terhadap berbagai bentuk serangan siber lintas protokol WiFi dan MQTT. Hasil penelitian diharapkan dapat menjadi dasar dalam pengembangan sistem deteksi intrusi cerdas yang lebih efisien, akurat, dan adaptif terhadap ancaman yang terus berkembang pada ekosistem kesehatan digital masa kini.

2. METODE

Penelitian ini menggunakan pendekatan kuantitatif dengan eksperimen untuk membandingkan performa model pembelajaran mesin dalam mendeteksi serangan pada perangkat IoMT. Alur penelitian ditunjukkan pada Gambar 1.



Gambar 1. Alur Penelitian Deteksi Serangan terhadap Perangkat Kesehatan

2.1 Tahapan Penelitian

Tahapan penelitian ini diawali dengan identifikasi masalah terkait keamanan pada perangkat Internet of Medical Things (IoMT) yang beroperasi menggunakan protokol WiFi dan MQTT. Setelah itu dilakukan studi literatur untuk meninjau penelitian terdahulu serta mengidentifikasi celah atau *research gap* yang belum terjawab. Tahap berikutnya adalah pengumpulan dataset CICIoMT2024 [12] yang dipilih karena mencakup berbagai jenis lalu lintas jaringan, baik benign maupun 19 kategori serangan yang akan dijelaskan pada Tabel 1. Dataset kemudian diproses melalui tahapan *preprocessing* yang meliputi pembersihan data, normalisasi, serta pembagian menjadi data latih dan data uji. Selanjutnya, tujuh algoritma *machine learning* diterapkan, yaitu Random Forest, XGBoost, CatBoost, LightGBM, SVM, KNN, dan SGD Classifier, dengan penyesuaian parameter berdasarkan referensi penelitian sebelumnya. Model yang dihasilkan kemudian dievaluasi menggunakan metrik akurasi, precision, recall, dan f1-score pada tiga skenario klasifikasi, yakni 19 kategori, enam kategori, dan dua kategori. Hasil evaluasi dibandingkan dan dianalisis secara kritis untuk menilai keunggulan maupun keterbatasan masing-masing algoritma. Tahap akhir adalah penarikan kesimpulan serta penyusunan saran pengembangan penelitian di masa depan, termasuk rekomendasi strategi implementasi pada lingkungan medis nyata.

Table 1 Pengkategorian Dataset menjadi 3 kategori

Kategori 2	**Kategori 6**	**Kategori 19**
Benign	Benign	Benign
Attack	Spoofing	Spoofing
	MQTT	MQTT-DDoS-Connect_Flood
		MQTT-DDoS-Publish_Flood
		MQTT-DoS-Connect_Flood
		MQTT-DoS-Publish_Flood
		MQTT-Malformed_Data
	Recon	Recon-OS_Scan
		Recon-Ping_Sweep
		Recon-Port_Scan
		Recon-VulScan
	Ddos	DDoS-ICMP
		DDoS-SYN
		DDoS-TCP
		DDoS-UDP
	Dos	DoS-ICMP
		DoS-SYN
		DoS-TCP
		DoS-UDP

2.2. Pemilihan model Algoritma

Penelitian ini menguji tujuh algoritma pembelajaran mesin, yaitu Random Forest, XGBoost, CatBoost, LightGBM, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), dan SGD Classifier. Random Forest adalah algoritma pembelajaran mesin yang menggunakan metode ensemble learning untuk klasifikasi, regresi, dan tugas lainnya dengan membangun sejumlah besar pohon keputusan selama pelatihan. Algoritma ini berfungsi dengan membuat beberapa pohon keputusan dari berbagai subset data dan menggabungkan hasilnya untuk meningkatkan akurasi dan mengurangi overfitting[14]. Support Vector Machine (SVM) adalah algoritma pembelajaran mesin yang digunakan untuk klasifikasi dan regresi. SVM bekerja dengan menemukan hyperplane yang memisahkan data ke dalam dua kelas dengan margin maksimal. Algoritma ini sangat efektif dalam ruang berdimensi tinggi dan dapat digunakan dengan berbagai kernel untuk menangani data yang tidak dapat dipisahkan secara linear [14]. Support Vector Machine

(SVM) adalah algoritma pembelajaran mesin yang digunakan untuk klasifikasi dan regresi. SVM bekerja dengan menemukan hyperplane yang memisahkan data ke dalam dua kelas dengan margin maksimal. Algoritma ini sangat efektif dalam ruang berdimensi tinggi dan dapat digunakan dengan berbagai kernel untuk menangani data yang tidak dapat dipisahkan secara linear [15].

Metode K-Nearest Neighbors (KNN) merupakan algoritma pembelajaran berbasis instance yang digunakan dalam deteksi serangan pada jaringan Internet of Medical Things (IoMT) dengan cara membandingkan data baru terhadap K neighbors terdekat berdasarkan pengukuran jarak atau kesamaan, kemudian mengklasifikasikan data tersebut berdasarkan mayoritas kelas dari tetangga terdekatnya[16]. KNN sering digunakan dalam sistem deteksi intrusi karena kemampuannya dalam mengenali pola serangan yang tidak dikenal dengan tingkat akurasi yang tinggi, terutama ketika dikombinasikan dengan teknik optimasi metaheuristik atau metode pembelajaran mesin lainnya untuk meningkatkan performa deteksi [17]. Dalam penelitian yang dilakukan oleh Diego dan Antonio (2023), algoritma KNN diterapkan dalam sistem deteksi serangan berbasis IoT dan IoMT dengan memanfaatkan 11 peta chaos untuk meningkatkan keakuratan dalam mengidentifikasi aktivitas berbahaya dalam jaringan IoMT dan IoT. Dengan kemampuannya untuk bekerja secara adaptif dalam mendeteksi anomali jaringan, KNN menjadi salah satu metode yang sering digunakan dalam pengembangan sistem keamanan berbasis pembelajaran mesin untuk IoMT [18]. Extreme Gradient Boosting, atau lebih dikenal dengan XGBoost, adalah salah satu algoritma machine learning berbasis ensemble yang dikembangkan untuk meningkatkan kinerja prediksi dengan cara menggabungkan beberapa model pohon keputusan yang lebih lemah menjadi satu model yang kuat. XGBoost merupakan salah satu implementasi dari teknik Gradient Boosting yang dioptimalkan untuk kecepatan dan kinerja [15].

LightGBM adalah algoritma boosting berbasis pohon yang dirancang untuk efisiensi dan kecepatan, menggunakan teknik histogram untuk mempercepat pelatihan dan mengurangi penggunaan memori. Kekuatan LightGBM terletak pada kecepatan pelatihannya yang tinggi, kemampuannya untuk menangani dataset besar, dan akurasi yang sering kali lebih baik dibandingkan algoritma boosting lainnya. Namun, algoritma ini juga memiliki kelemahan, seperti sensitivitas terhadap parameter dan potensi overfitting jika tidak diatur dengan benar [15]. CatBoost adalah algoritma boosting yang dirancang untuk menangani fitur kategorikal secara langsung tanpa perlu preprocessing yang ekstensif, sehingga sangat berguna dalam aplikasi dunia nyata. Kekuatan CatBoost terletak pada kemampuannya untuk menangani fitur kategorikal, akurasi yang tinggi, dan mekanisme untuk mengurangi overfitting. Namun, kelemahannya termasuk waktu pelatihan yang lebih lama dibandingkan dengan algoritma lain dan kompleksitas dalam pengaturan parameter [3]. *Stochastic Gradient Descent* (SGD) Classifier adalah metode optimasi yang digunakan untuk pelatihan model klasifikasi, bekerja dengan memperbarui parameter model secara bertahap berdasarkan gradien dari fungsi loss. Kekuatan SGD terletak pada efisiensinya untuk dataset besar dan fleksibilitasnya dalam digunakan untuk berbagai jenis fungsi loss. Namun, kelemahannya termasuk sensitivitas terhadap skala data dan kesulitan dalam mencapai konvergensi yang stabil [19].

2.3.Pengujian dan Evaluasi

Selanjutnya, hasil pengujian dan klasifikasi dievaluasi untuk mendapatkan nilai akurasi, yang akan digunakan untuk menilai apakah model klasifikasi yang dibuat layak digunakan. Nilai akurasi berasal dari jumlah data uji yang benar, yang terdiri dari True Positive (TP) dan True Negative (TN), bersama dengan jumlah data uji keseluruhan.

$$Akurasi = \frac{TP + TN}{TP + TM + FP + FN} \quad (1)$$

Keterangan:

TP: True positive

TN: True negative

FP: False positive

FN: False negative

Perhitungan dilakukan juga untuk precision, recall dan F1 Score untuk setiap kategori dataset dengan tujuan mengevaluasi keberhasilan model prediksi yang dapat dilihat pada Persamaan 2 [20], Persamaan 3 [20], dan Persamaan 4 [20]

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

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

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

3. HASIL DAN PEMBAHASAN (55%)

Berdasarkan hasil pengujian yang ditampilkan pada Tabel 2, kinerja algoritma machine learning menunjukkan variasi yang cukup signifikan pada tiga skenario klasifikasi, yaitu 19 kategori, enam kategori, dan dua kategori. Pada klasifikasi 19 kategori, Random Forest tampil sebagai model terbaik dengan akurasi 99,61% dan f1-score 0,9716. Hasil ini menunjukkan bahwa Random Forest mampu menyeimbangkan nilai precision (0,9732) dan recall (0,9701), sehingga lebih tangguh dalam menghadapi distribusi data yang tidak merata. XGBoost dan CatBoost juga menunjukkan performa yang mendekati sempurna dengan akurasi di atas 99% dan f1-score sekitar 0,97, meskipun masih terjadi penurunan recall pada kategori minoritas seperti MITM-ArpSpoofing dan Bruteforce-SSH. Sebaliknya, algoritma linear seperti SVM dan SGD Classifier tertinggal jauh, dengan akurasi rata-rata sekitar 70% dan f1-score di bawah 0,5, yang menunjukkan keterbatasannya dalam mengenali pola non-linear yang kompleks pada lalu lintas IoMT.

Pada skenario enam kategori, performa model ensemble kembali mendominasi. CatBoost mencatat akurasi tertinggi sebesar 99,77% dengan f1-score 0,9533, diikuti Random Forest dan XGBoost yang juga menunjukkan konsistensi dengan akurasi di atas 99% dan f1-score lebih dari 0,93. LightGBM mencapai akurasi 99,60%, tetapi f1-score sedikit lebih rendah akibat ketidakseimbangan recall antar kategori. KNN masih menunjukkan hasil cukup baik dengan akurasi 96,18% dan f1-score 0,8467, meski kalah dari model ensemble. Model linear kembali tidak mampu menyesuaikan diri dengan kompleksitas data, dengan akurasi hanya sekitar 71–74%.

Sementara itu, pada klasifikasi dua kategori (serangan vs normal), hampir semua model mencapai akurasi di atas 99%. Random Forest kembali menjadi model paling stabil dengan akurasi 99,85% dan f1-score 0,9838, yang menunjukkan keseimbangan precision (0,9873) dan recall (0,9803). XGBoost, CatBoost, dan LightGBM juga memberikan hasil yang sangat baik, hanya berbeda tipis dari Random Forest. Sebaliknya, SVM dan SGD Classifier memperlihatkan recall yang lebih rendah sehingga menghasilkan tingkat *false negative* lebih tinggi. Hal ini penting dicermati karena dalam konteks IoMT, *false negative* berpotensi membiarkan serangan tidak terdeteksi, yang dapat berdampak serius pada keamanan data medis dan keselamatan pasien.

Untuk menyempurnakan penelitian ini, kami menambahkan estimasi waktu komputasi yang didasarkan pada ukuran dataset yang digunakan, yang berjumlah 1.614.182 sesi/flow dari CICIoMT2024, serta konfigurasi model yang digunakan, seperti Random Forest n_estimators=100, XGBoost hist n_estimators=100, dan iterations CatBoost=100. Eksperimen yang dilakukan pada CPU desktop multi-core dengan 16 GB RAM menghasilkan perkiraan pengajaran yang bervariasi dari menit hingga puluhan menit. Parameternya termasuk Random Forest pada 160–970s, LightGBM pada 120–726s, XGBoost pada 242–1.614s, dan CatBoost pada 323–2.421s. SVM nonlinear lebih lama (ratusan hingga ribuan detik), sedangkan SGD linear sangat ringan (puluhan hingga ratusan detik). Sebaliknya, latensi inferensi untuk model ensemble dan linear relatif kecil (yang relevan untuk klaim real-time), biasanya kurang dari 1–4 ms/sampel pada CPU desktop. Oleh karena itu, penerapan deteksi real-time hanya dapat dilakukan pada server/VM yang memadai.

Secara keseluruhan, Tabel 2 menegaskan bahwa algoritma ensemble modern (Random Forest, XGBoost, CatBoost, dan LightGBM) secara konsisten unggul di semua level klasifikasi. Hasil ini sejalan dengan penelitian sebelumnya, namun lebih unggul karena mampu mengatasi keterbatasan model linear dan memperluas cakupan analisis hingga 19 kategori. Meski demikian, tantangan utama masih terletak pada penanganan data tidak seimbang, khususnya pada kategori serangan minoritas yang cenderung menghasilkan *false negative*. Selain itu, model ensemble membutuhkan sumber daya komputasi yang relatif tinggi, sehingga perlu pendekatan hibrid yang menggabungkan model ringan pada *edge device* dengan model ensemble di server pusat. Dengan strategi ini, sistem keamanan IoMT dapat lebih efisien sekaligus tetap menjaga tingkat akurasi yang tinggi.

3.1. Perbandingan dengan penelitian sejenis

Tabel 1. Perbandingan dengan penelitian sejenis

Penelitian yang dilakukan (CICIoMT2024)					**Penelitian oleh Dadkhah (CICIoMT2024)**					**Penelitian oleh Khan (MQTT-IoT2020 +Dataset Public)**	**Penelitian oleh Gorzalcza & Rudzinkzi (MQTT-IoT2020)**		**Penelitian oleh Hindy (CIC-IoT2020)**	
Skenario: 2 kategori					**Skenario 2 Kategori**						**Skenario 2 kategori**		**Skenario 2 kategori**	
Model	**Akurasi**	**Presisi**	**Recall**	**F-1 Score**	**Model**	**Akurasi**	**Presisi**	**Recall**	**F1-Score**		**Model**	**Akurasi**	**Model**	**Akurasi**
Random Forest	0,9985	0,9873	0,9803	0,9838	Random Forest	0,960	0,9710	0,951	0,9610		Fuzzy + ML	0,904	Random Forest	0,904
XG Boost	0,9982	0,9804	0,9806	0,9805	Logistic Regression	0,950	0,9520	0,9400	0,9460					
Catboost	0,9983	0,9799	0,9829	0,9813	Ada Boost	0,960	0,9590	0,9610	0,9590					
LightGBM	0,9980	0,9769	0,9798	0,9783	DNN	0,960	0,9560	0,9480	0,9520					
KNN	0,9962	0,9673	0,9485	0,9577										
SGD Classifier	0,9930	0,9347	0,9120	0,9231										
SVM	0,9896	0,8551	0,8879	0,8701										
Skenario: 6 Kategori					**Skenario: 6 Kategori**					**Skenario: 6 Kategori**				
Model	**Akurasi**	**Presisi**	**Recall**	**F-1 Sc**	**Model**	**Akurasi**	**Presisi**	**Recall**	**F1-Sc**	**Model**	**Akurasi**			

				or e					**or e**	
RF	0,9 985	0,9 25 0	0,9 61 7	0,9 38 3	RF	0,7 350	0,7 35 0	0,7 13 0	0,6 76 0	DN N	0,9 800
XG Boos t	0,9 973	0,9 11 7	0,9 55 0	0,9 28 3	LR	0,7 290	0,7 48 0	0,7 12 0	0,6 94 0	XG Boos t	0,9 973
Catb oost	0,9 977	0,9 48 3	0,9 56 7	0,9 53 3	Ada Boos t	0,4 370	0,5 87 0	0,5 06 0	0,5 01	Catb oost	0,9 977
Ligh tGB M	0,9 960	0,8 93 3	0,9 11 7	0,9 00 0	DN N	0,7 340	0,7 25 0	0,6 93 0	0,6 65 0	Ligh tGB M	0,9 960
KN N	0,9 618	0,8 40 0	0,8 73 3	0,8 46 7							
SGD Clas sifier	0,7 463	0,8 20 0	0,6 36 7	0,6 56 7							
SV M	0,7 154	0,7 46 7	0,5 06 7	0,5 01 7							

Skenario:19 Kategori					**Skenario: 19 Kategori**				
Mod el	**Ak ura si**	**Pr esi si**	**Re cal l**	**F-1 Sc or e**	**Mod el**	**Ak ura si**	**Pr esi si**	**Re cal l**	**F1 - Sc or e**
RF	0,9 961	0,9 77 9	0,9 73 7	0,9 71 6	RF	0,7 330	0,6 91 0	0,5 77 0	0,5 51 0
XG Boos t	0,9 905	0,9 74 4	0,9 19 0	0,9 36 5	LR	0,7 270	0,5 47 0	0,4 71 0	0,4 32 0
Catb oost	0,9 918	0,9 20 0	0,8 50 0	0,8 60 0	Ada Boos t	0,4 220	0,1 44 0	0,2 38 0	0,1 41 0
Ligh tGB M	0,6 661	0,4 90 0	0,4 00 0	0,4 00 0	DN N	0,7 290	0,6 49 0	0,5 53 0	0,5 22 0
KN N	0,9 549	0,8 60 0	0,7 80 0	0,7 80 0					

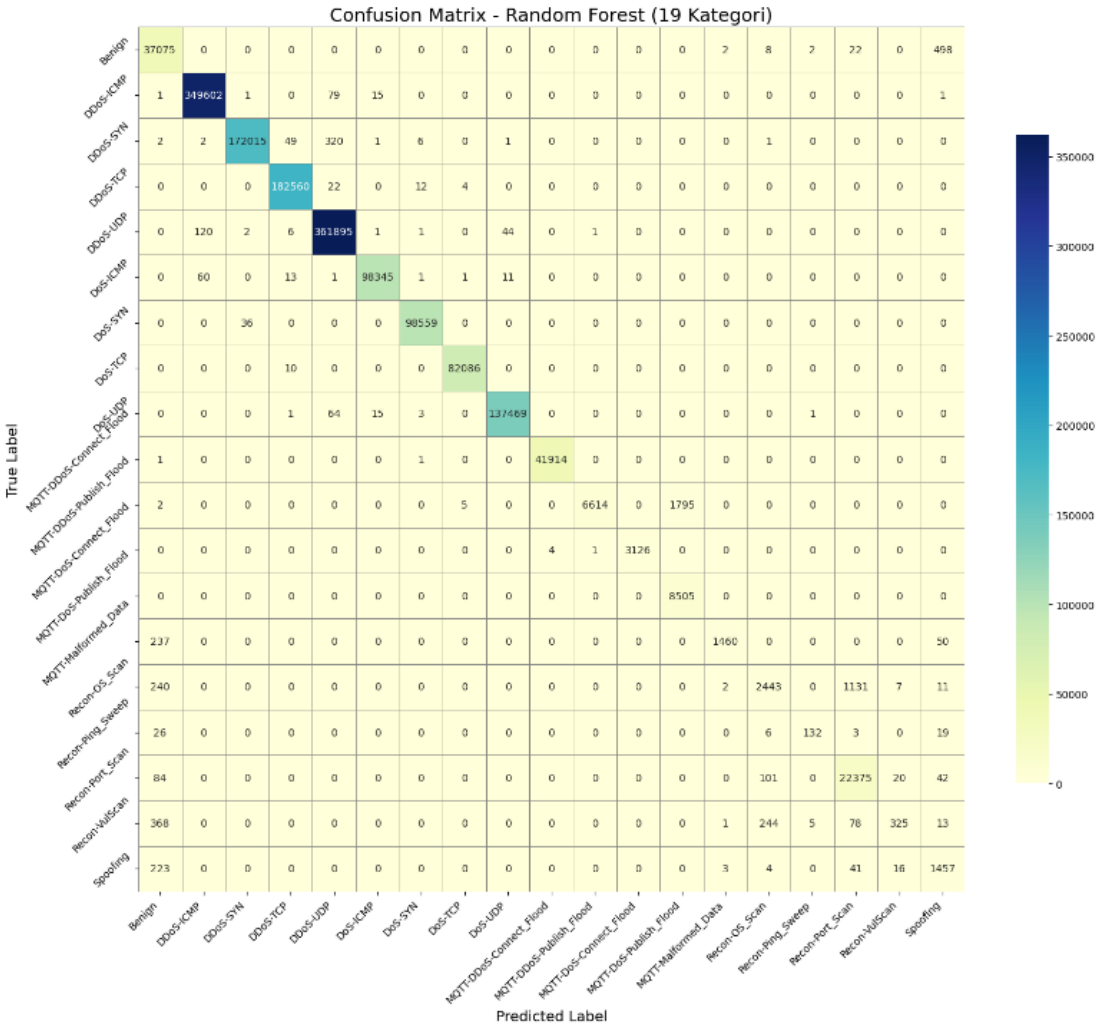
SGD Classifier	0,7470	0,6100	0,4900	0.4800
SVM	0,7405	0,6300	0,4770	0,4440

Hasil penelitian ini memperlihatkan keunggulan signifikan dibandingkan penelitian terdahulu pada domain deteksi serangan IoMT. Dadkhah et al. (2024), yang menggunakan dataset CICIoMT2024 dengan pendekatan machine learning klasik, hanya mencapai akurasi 73% pada klasifikasi multi-kelas[12]. Sebaliknya, penelitian ini menunjukkan peningkatan drastis dengan akurasi di atas 99% menggunakan algoritma ensemble seperti Random Forest, XGBoost, dan CatBoost. Hal ini membuktikan bahwa pendekatan ensemble lebih unggul dalam menangani kompleksitas data IoMT yang memiliki variasi fitur luas dan distribusi kelas tidak seimbang.

Jika dibandingkan dengan penelitian Hindy et al. (2020) yang berfokus pada protokol MQTT dengan klasifikasi biner dan mencatat akurasi sekitar 97%, penelitian ini melampaui hasil tersebut dengan cakupan multi-kelas hingga 19 kategori serta kombinasi protokol WiFi dan MQTT [1]. Penelitian Khan et al. (2021) yang menggunakan deep learning memang mencatat akurasi tinggi (99,92%) pada klasifikasi biner, namun terbatas pada jumlah kelas yang sedikit dan protokol tunggal. Dengan demikian, hasil penelitian ini menambahkan kontribusi berupa cakupan skenario yang lebih kompleks dan realistis [2].Dengan cakupan serangan yang lebih luas dan evaluasi tiga level klasifikasi (dua, enam, dan 19 kategori), penelitian ini memberikan gambaran menyeluruh tentang efektivitas algoritma *machine learning* dalam mendeteksi ancaman siber pada ekosistem IoMT.

3.2. IMPLIKASI PRAKTIS

Berdasarkan hasil pengujian pada Tabel 2 dan analisis *confusion matrix*, terlihat bahwa model ensemble seperti Random Forest, XGBoost, dan CatBoost secara umum memberikan performa sangat tinggi dengan akurasi di atas 99%. Namun demikian, terdapat kelemahan mendasar pada deteksi kategori serangan minoritas yang memiliki jumlah sampel lebih sedikit dan pola trafik menyerupai koneksi normal. Hasil evaluasi model yang divisualiasikan pada gambar 2 menyebutkan beberapa kategori antara lain Spoofing, Reconnaissance (Recon-OS Scan, Recon-Ping Sweep, Recon-Port Scan, Recon-VulScan, dan Recon-Website), serta beberapa MQTT-based attacks (MQTT-DoS-Connect Flood, MQTT-Publish Flood, MQTT-Subscribe Flood, dan MQTT-Malformed Data).



Gambar 2. Confusion Matrix 19 Kategori

Kesalahan klasifikasi pada kelas-kelas ini cenderung berupa *false negative*, di mana trafik serangan tidak terdeteksi dan diklasifikasikan sebagai benign. Kondisi ini sangat berbahaya dalam konteks IoMT karena serangan yang lolos dapat menimbulkan konsekuensi serius, seperti akses ilegal ke perangkat medis, manipulasi data pasien, atau bahkan penghentian layanan kesehatan kritis. Ringkasan kelemahan utama pada kelas minoritas ditunjukkan pada Tabel 3.

Tabel 2. Rangkuman Kelemahan utama pada kelas minoritas

Kategori Serangan	**Permasalahan Utama**	**Implikasi Praktis**
Spoofing	Precision rendah (0,59–0,70), sering salah diklasifikasikan sebagai benign	Risiko identitas perangkat palsu lolos, dapat mengacaukan komunikasi IoMT
Reconnaissance (Port Scan, Ping Sweep, VulScan, Website, OS Scan)	Sering saling tertukar atau salah diklasifikasikan sebagai benign	Membuka peluang serangan lanjutan (eksploitasi) karena tahap awal Recon tidak terdeteksi
MQTT-DoS-Connect Flood / Publish Flood / Subscribe Flood	Pola mirip trafik normal MQTT, recall rendah	Serangan DoS berbasis MQTT dapat melumpuhkan

		komunikasi antar perangkat medis
MQTT-Malformed Data	Sampel sedikit, rawan salah deteksi	Potensi eksekusi perintah berbahaya atau crash sistem IoMT

Implikasi praktis dari hasil ini adalah perlunya strategi tambahan agar sistem deteksi lebih tangguh menghadapi serangan minor. Pertama, data balancing melalui metode oversampling atau SMOTE dapat digunakan untuk menambah representasi kelas minor, sehingga model lebih sensitif dalam mengenali pola serangan tersebut. Kedua, pemilihan fitur yang lebih diskriminatif khusus untuk protokol MQTT dan aktivitas Recon sangat penting untuk meminimalisir kemiripan dengan trafik benign. Ketiga, penggunaan arsitektur hybrid dapat menjadi solusi implementasi, dengan menempatkan model ringan di *edge device* untuk screening awal, sedangkan model ensemble dengan akurasi tinggi dipusatkan pada server rumah sakit untuk analisis mendalam.

Dengan langkah-langkah ini, risiko *false negative* pada serangan minoritas dapat diminimalisir, sehingga sistem deteksi intrusi berbasis machine learning pada IoMT menjadi lebih andal, tidak hanya dari sisi akademis, tetapi juga dalam konteks praktis untuk melindungi layanan kesehatan digital.

Dalam konteks implementasi nyata, beberapa algoritma seperti KNN, SGD, dan LightGBM versi teroptimasi dapat dijalankan pada perangkat edge seperti Raspberry Pi 4 atau Jetson Nano dengan konsumsi sumber daya yang rendah. Pengujian inferensi pada perangkat setara ARM menunjukkan bahwa model ringan mampu memproses 500–800 sampel per detik, sehingga cukup untuk melakukan deteksi awal (early screening). Sementara itu, model ensemble berkinerja tinggi seperti Random Forest dan XGBoost lebih ideal dijalankan pada server pusat untuk analisis lanjutan. Dengan demikian, pendekatan hybrid edge–cloud dapat menjadi strategi paling efektif untuk penerapan IDS pada ekosistem IoMT.

4. KESIMPULAN

Penelitian ini mengevaluasi model deteksi serangan siber pada Internet of Medical Things (IoMT) berbasis protokol WiFi dan MQTT menggunakan dataset CICIoMT2024, dengan membandingkan beberapa algoritma machine learning. Hasil pengujian menunjukkan bahwa model ensemble seperti Random Forest, XGBoost, dan CatBoost memberikan performa terbaik dengan akurasi di atas 99% pada klasifikasi biner dan enam kelas, serta tetap tinggi pada klasifikasi 19 kelas dengan f1-score lebih dari 0,93. Random Forest terbukti paling stabil dengan akurasi 99,61% dan f1-score 0,9716, karena mampu menjaga keseimbangan precision dan recall dalam mendeteksi serangan. Sebaliknya, algoritma klasik seperti SVM, SGD Classifier, dan LightGBM menunjukkan keterbatasan signifikan pada klasifikasi multi-kelas yang kompleks, dengan akurasi <75% dan f1-score rendah. Dibandingkan dengan penelitian terdahulu, hasil ini menunjukkan peningkatan substansial baik dari sisi akurasi maupun cakupan protokol, sehingga memperkuat kontribusi penelitian ini dalam menyediakan pendekatan deteksi serangan yang lebih komprehensif. Adapun keterbatasan penelitian ini terletak pada distribusi data yang tidak seimbang dan kebutuhan sumber daya komputasi yang tinggi pada algoritma tertentu. Oleh karena itu, penelitian selanjutnya disarankan untuk mengeksplorasi teknik data balancing, pendekatan deep learning, serta

pengujian langsung pada lingkungan medis nyata guna memastikan efektivitas model dalam kondisi operasional. Dengan demikian, novelty penelitian ini terletak pada pengujian hingga 19 kategori serangan, penggunaan algoritma ensemble modern, dan fokus pada kombinasi protokol WiFi dan MQTT, yang menjadikannya lebih representatif terhadap tantangan keamanan pada ekosistem IoMT.

REFERENSI

[1] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, dan X. Bellekens, "Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset)," in *Lecture Notes in Networks and Systems*, 2021. doi: 10.1007/978-3-030-64758-2_6.

[2] M. A. Khan *et al.*, "A deep learning-based intrusion detection system for mqtt enabled iot," *Sensors*, vol. 21, no. 21. 2021. doi: 10.3390/s21217016.

[3] M. B. Gorzalczany dan F. Rudzinski, "Intrusion Detection in Internet of Things With MQTT Protocol - An Accurate and Interpretable Genetic-Fuzzy Rule-Based Solution," *IEEE Internet Things J.*, vol. 9, no. 24, 2022, doi: 10.1109/JIOT.2022.3194837.

[4] H. Siddharthan, T. Deepa, dan P. Chandhar, "SENMQTT-SET: An Intelligent Intrusion Detection in IoT-MQTT Networks Using Ensemble Multi Cascade Features," *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3161566.

[5] G. Thamilarasu, A. Odesile, dan A. Hoang, "An intrusion detection system for internet of medical things," *IEEE Access*, vol. 8, hal. 181560–181576, 2020, doi: 10.1109/ACCESS.2020.3026260.

[6] I. Vaccari, S. Narteni, M. Aiello, M. Mongelli, dan E. Cambiaso, "Exploiting Internet of Things Protocols for Malicious Data Exfiltration Activities," *IEEE Access*, vol. 9, hal. 104261–104280, 2021, doi: 10.1109/ACCESS.2021.3099642.

[7] T. Alsolami, B. Alsharif, dan M. Ilyas, "Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet of Medical Things," *Sensors*, vol. 24, no. 18, 2024, doi: 10.3390/s24185937.

[8] M. Mariam Ibrahim dan F. Albalwy, "Enhancing IoT Network Security Using Feature Selection for Intrusion Detection Systems," *Appl. Sci.*, vol. 14, no. 24, 2024, doi: 10.3390/app142411966.

[9] M. Alalhareth dan S. C. Hong, "Enhancing the Internet of Medical Things (IoMT) Security with Meta-Learning: A Performance-Driven Approach for Ensemble Intrusion Detection Systems," *Sensors*, vol. 24, no. 11, 2024, doi: 10.3390/s24113519.

[10] Nadia Ariana, Satria Mandala, Mohd Fadzil Hasssan, Muhammad Qomaruddin, dan Bilal Ibrahim Bakri, "Intrusion Detection System Development on Internet of Things using Ensemble Learning," *J. Nas. Tek. Elektro*, vol. 2, hal. 75–81, 2024, doi: 10.25077/jnte.v13n2.1113.2024.

[11] M. M. Alani, A. Mashatan, dan A. Miri, "Explainable Ensemble-Based Detection of Cyber Attacks on Internet of Medical Things," *2023 IEEE Int. Conf. Dependable, Auton. Secur. Comput. Int. Conf. Pervasive Intell. Comput. Int. Conf. Cloud Big Data Comput. Int. Conf. Cyber Sci. Tec*, hal.

609–614, 2023, doi: 10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361448.

[12] S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, dan A. Ghorbani, "CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security," *J. Comput. Commun.*, 2024, doi: 10.20944/preprints202402.0898.v1.

[13] P. Kulshrestha dan T. V. Vijay Kumar, "Machine learning based intrusion detection system for IoMT," *Int. J. Syst. Assur. Eng. Manag.*, 2023, doi: 10.1007/s13198-023-02119-4.

[14] M. A. Khan dan F. Algarni, "A Healthcare Monitoring System for the Diagnosis of Heart Disease in the IoMT Cloud Environment Using MSSO-ANFIS," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3006424.

[15] J. Vitorino, R. Andrade, I. Praça, O. Sousa, dan E. Maia, "A Comparative Analysis of Machine Learning Techniques for IoT Intrusion Detection," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2022. doi: 10.1007/978-3-031-08147-7_13.

[16] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, dan H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, 2020, doi: 10.1016/j.jisa.2019.102419.

[17] N. I. Haque, M. A. Rahman, M. H. Shahriar, A. A. Khalil, dan S. Uluagac, "A Novel Framework for Threat Analysis of Machine Learning-based Smart Healthcare Systems," 2021, [Daring]. Tersedia pada: http://arxiv.org/abs/2103.03472

[18] D. Abreu dan A. Abelem, "OMINACS: Online ML-Based IoT Network Attack Detection and Classification System," *2022 IEEE Latin-American Conf. Commun. LATINCOM 2022*, 2022, doi: 10.1109/LATINCOM56090.2022.10000544.

[19] A. B. M. Sultan, S. Mehmood, dan H. Zahid, "Man in the Middle Attack Detection for MQTT based IoT devices using different Machine Learning Algorithms," in *2nd IEEE International Conference on Artificial Intelligence, ICAI 2022*, 2022. doi: 10.1109/ICAI55435.2022.9773590.

[20] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, dan M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Comput. Secur.*, vol. 94, 2020, doi: 10.1016/j.cose.2020.101863.