Jurnal InComTech April 2025-Roymond Chandra P.docx

by - -

Submission date: 06-Feb-2025 01:02PM (UTC+0530)
Submission ID: 2581082935
File name: Jurnal_InComTech_April_2025-Roymond_Chandra_P.docx (303.11K)
Word count: 2534
Character count: 16450

InComTech: Jurnal Telekomunikasi dan Komputer
vol.xx, no.x, Agustus 2022, xxx-xxx
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] *FakultasTeknik, Magister Teknik Informatika, Universitas Amikom, Jl. Ring Road Utara, Condong Catur, Sleman, Yogyakarta, Indonesia*

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

Abstrak **:**
Perangkat kesehatan yang tergabung dalam Internet of Medical Things (IoMT) rentan terhadap serangan siber, terutama saat menggunakan protokol komunikasi seperti WiFi dan MQTT. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis serangan pada perangkat IoMT serta mengembangkan model deteksi yang efektif berbasis machine learning. Metode yang digunakan meliputi pengumpulan data dari dataset terbuka, preprocessing data, dan penerapan berbagai algoritma machine learning seperti Random Forest, SVM, KNN, LightGBM, SGD Classifier, CatBoost, dan XGBoost. Hasil pengujian menunjukkan model yang dikembangkan memiliki tingkat akurasi tinggi, yakni 99,5% untuk deteksi dua kategori serangan, 91,5% untuk enam kategori, dan 86,9% untuk sembilan belas kategori. Temuan ini membuktikan bahwa machine learning dapat meningkatkan deteksi serangan siber pada perangkat medis secara signifikan. Penelitian ini memberikan kontribusi penting bagi keamanan IoMT dengan menerapkan teknik machine learning yang canggih. Selain itu, studi ini menekankan pentingnya inovasi dalam mendeteksi serangan siber serta memberikan rekomendasi untuk pengembangan algoritma yang lebih efisien di masa depan.

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

Riwayat Artikel:
Received Jun x, 20xx
Revised Nov x, 20xx
Accepted Dec x, 20xx

DOI:
10.22441/incomtech.v10i3.7777

1. PENDAHULUAN

Pesatnya perkembangan teknologi Internet of Things (IoT) telah memungkinkan perangkat kesehatan untuk terhubung dalam jaringan yang luas, menciptakan konsep yang dikenal sebagai Internet of Medical Things (IoMT) [1]. Perangkat IoMT, seperti monitor pasien, pompa insulin, dan perangkat wearable, memainkan

peran signifikan dalam meningkatkan layanan kesehatan melalui pemantauan real-time dan pengambilan keputusan yang lebih cepat [2]. Namun, semakin banyaknya perangkat yang terhubung juga membuka peluang risiko keamanan, khususnya dalam protokol komunikasi seperti WiFi dan Message Queuing Telemetry Transport (MQTT) [3].

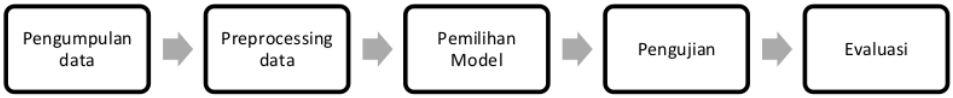
Protokol MQTT, yang dirancang untuk komunikasi ringan antar perangkat dengan sumber daya terbatas, meskipun efisien, memiliki kelemahan keamanan yang signifikan. Menurut laporan Badan Siber dan Sandi Negara (BSSN), jumlah anomali pada perangkat IoT di Indonesia telah mencapai 80.319 kasus pada tahun 2024 [4]. Kerentanan pada protokol ini dapat dimanfaatkan dalam serangan seperti Denial of Service (DoS) dan Man-in-the-Middle (MiTM), yang berpotensi membahayakan integritas dan kerahasiaan data medis [5].

Penelitian sebelumnya menunjukkan bahwa pendekatan berbasis machine learning dan deep learning memiliki potensi besar dalam mendeteksi serangan tersebut. Metode ini tidak hanya meningkatkan akurasi deteksi hingga lebih dari 99%[6] tetapi juga menawarkan pendekatan yang lebih adaptif dan efisien untuk mendeteksi anomali jaringan[5]–[7]. Namun, tantangan utama tetap terletak pada penerapan solusi ini secara real-time di perangkat medis dengan sumber daya terbatas [8].

Penelitian ini bertujuan untuk mengembangkan model machine learning yang efisien dan akurat untuk mendeteksi berbagai jenis serangan pada perangkat IoMT yang menggunakan WiFi dan protokol MQTT. Dengan pendekatan ini, diharapkan dapat tercipta ekosistem IoMT yang lebih aman dan andal, sehingga meningkatkan kepercayaan terhadap teknologi dalam dunia kesehatan.

2. METODE

Penelitian ini menggunakan pendekatan kuantitatif dengan eksperimen untuk membandingkan performa model pembelajaran mesin dalam mendeteksi serangan pada perangkat IoMT. Alur metode penelitian dapat dirinci sebagai berikut:



Gambar 1 Alur Penelitian Deteksi Serangan

2.1 Tahapan Penelitian

2.1.1 Pengumpulan Data

Dataset yang digunakan adalah **CIC IoMT 2024** [9], yang dikembangkan oleh Canadian Institute for Cybersecurity. Dataset ini mencakup data normal (benign) dan data serangan (DoS, DDoS, recon, spoofing, dan serangan berbasis MQTT). Dataset tersebut dibagi menjadi beberapa kategori, seperti:

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

2.1.2 Preprocessing Data

Pada tahap ini dilakukan pembersihan dan pengolahan data sebagai berikut:

- Memuat dan Menggabungkan Dataset: Dataset terdiri dari data latih (train) dan data uji (test) yang disimpan dalam format .csv dalam dua folder (train/ dan test/).
- Memberikan Label pada Data.
- Pemisahan Fitur (X) dan Target (y): Fitur (X): Semua kolom kecuali Attack_Type (label) dan file (nama file) dan Target (y): Kolom Attack_Type, yang berisi label kategori serangan.
- Encoding Label Kategori: mengubah kategori serangan (teks) menjadi nilai numerik. Encoding ini diperlukan agar algoritma pembelajaran mesin bisa memproses label dengan benar.

- Membagi Data Latih dan Validasi: train_test_split() membagi 20% data latih menjadi data validasi bertujuannya adalah untuk menguji model sebelum diterapkan ke data uji (test set). Dan random_state=42 memastikan hasil pembagian dataset tetap konsisten setiap kali dijalankan.
- Normalisasi Data: StandardScaler() melakukan normalisasi (standarisasi) dengan mengonversi data agar memiliki mean = 0 dan standar deviasi = 1. Bertujuan untuk menghindari dominasi fitur dengan skala besar serta meningkatkan stabilitas dan performa model pembelajaran mesin. fit_transform() digunakan untuk data latih, sedangkan transform() digunakan untuk data validasi dan uji agar tetap sesuai dengan skala yang sama.

2.1.3 Pemilihan Model

2.1.3.1 Random Forest

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[10].

2.1.3.2 K-Nearest Neighbors

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 [11]. 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 [12]. 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 [13].

2.1.3.3 Support Vector Machine

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].

2.1.3.4 LightGBM

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 [7].

2.1.3.5 Extreme Gradient Boosting (XGBoost)

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 [7].

2.1.3.6 Catboost

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 [8].

2.1.3.7 Stochastic Gradient Descent Classifier

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 [14].

2.1.4 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.

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

Keterangan:
TP: True positive
TN: True negative
FP: False positive
FN: False negative

Perhitungan dilakukan juga untuk precision, recall dan F1 Score untuk setiap kelas jenis dongeng dengan tujuan mengevaluasi keberhasilan model prediksi yang dapat dilihat pada Persamaan 2 [15], Persamaan 3 [15], dan Persamaan 4 [15].

$$Precision = \frac{TP}{TP + FP} \times 100\% \quad (2)$$

$$Recall = \frac{TP}{TP + FN} \times 100\% \quad (3)$$

$$F1 = \frac{2\ x\ Recall\ x\ Precision}{Recall + Precision} \quad (4)$$

3. HASIL DAN PEMBAHASAN (55%)

3.1. Hasil pengujian Penyerangan Siber yang dibagi menjadi 19 kategori

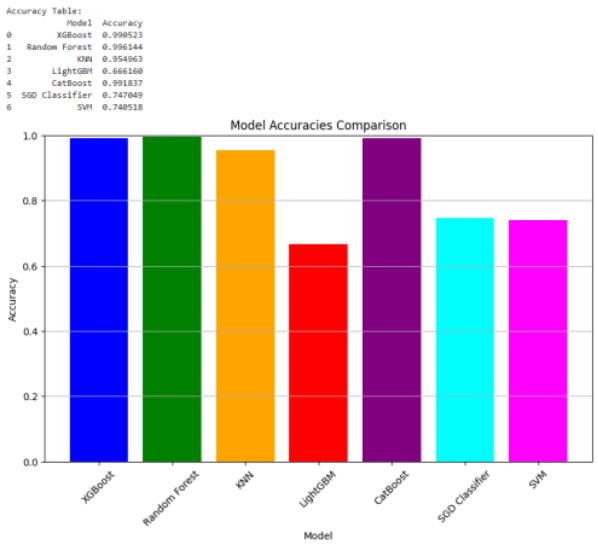
Berdasarkan eksperimen yang bertujuan untuk mengevaluasi kinerja berbagai model pembelajaran mesin dalam mendeteksi serangan pada jaringan Internet of Medical Things (IoMT) yang dibagi menjadi 19 ketegori sesuai dengan tabel 1 diatas. Model yang diuji termasuk XGBoost, Random Forest, K-Nearest Neighbors (KNN), LightGBM, CatBoost, SGD Classifier, dan Support Vector Machine (SVM). Hasil ditunjukan pada tabel 2 bahwa Random Forest memiliki akurasi tertinggi sebesar 99.61%, diikuti oleh CatBoost (99.18%) dan XGBoost (99.95%), sementara KNN memiliki akurasi 95.50%, yang masih dianggap tinggi tetapi lebih rendah dibandingkan dengan model berbasis ensemble. Model LightGBM, SGD Classifier, dan SVM memiliki kinerja yang lebih rendah, dengan akurasi di bawah 75%.

Untuk mengukur efektivitas model dalam mendeteksi serangan, digunakan classification report yang mencakup metrik precision, recall, dan f1-score. Beberapa hasil penting yang ditemukan dalam evaluasi:

- Random Forest memiliki f1-score tertinggi, menunjukkan kemampuannya dalam mengenali pola serangan dengan baik.
- XGBoost juga memiliki performa tinggi, tetapi sedikit lebih rendah dibandingkan Random Forest.
- KNN cukup baik dalam klasifikasi serangan, tetapi lebih rentan terhadap data yang memiliki distribusi tidak seimbang.
- LightGBM dan SVM menunjukkan f1-score rendah, yang mengindikasikan kelemahan dalam menangani variasi data yang kompleks.

Table 2 . Hasil Perbandingan antar model dalam 19 kategori

Nama Model	Akurasi (%)	Precision	Recall	F1-Score
Random Forest	99.61	1.00	1.00	1.00
CatBoost	99.18	1.00	1.00	1.00
XGBoost	99.05	1.00	0.99	1.00
KNN	95.50	0.98	0.97	0.96
SGD Classifier	74.70	0.88	0.86	0.87
SVM	74.05	0.83	0.91	0.81
LightGBM	66.62	0.66	0.66	0.66



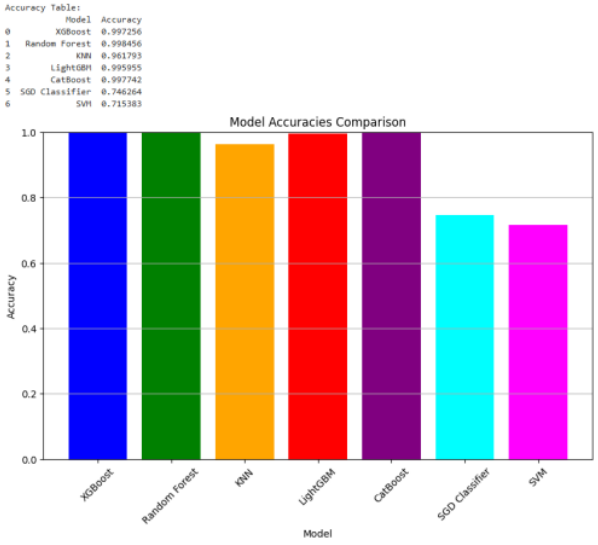
Gambar 2 Grafik Perbandingan Antar Model Pada 19 Kategori

3.2 Hasil pengujian Penyerangan Siber yang dibagi menjadi 6 kategori

Berdasarkan eksperimen yang bertujuan untuk mengevaluasi kinerja berbagai model pembelajaran mesin dalam mendeteksi serangan pada jaringan Internet of Medical Things (IoMT) yang dibagi menjadi 6 ketegori sesuai dengan tabel 1 diatas. Model yang diuji termasuk XGBoost, Random Forest, K-Nearest Neighbors (KNN), LightGBM, CatBoost, SGD Classifier, dan Support Vector Machine (SVM). Hasil ditunjukan pada tabel 3 bahwa Random Forest memiliki akurasi tertinggi sebesar 99.8 %, diikuti dengan Catboost dan XGBoosts keduanya memiliki akurasi 99.7%, lalu LightGBM dengan 99.5% dan KNN 96.1% sedangkan untuk model SGD Classifier dan SVM memiliki kinerja yang rendah yaitu 74.6% dan 71.5%.

Table 3 Hasil Perbandingan antar model dalam 6 kategori

Nama Model	Akurasi (%)	Precision	Recall	F1-Score
Random Forest	99.8	0.97	0.98	0.97
CatBoost	99.7	0.95	0.96	0.95
XGBoost	99.7	0.91	0.95	0.93
LightGBM	99.5	0.89	0.91	0.90
KNN	96.1	0.84	0.87	0.85
SGD Classifier	74.6	0.82	0.64	0.66
SVM	71.5	0.69	0.72	0.61



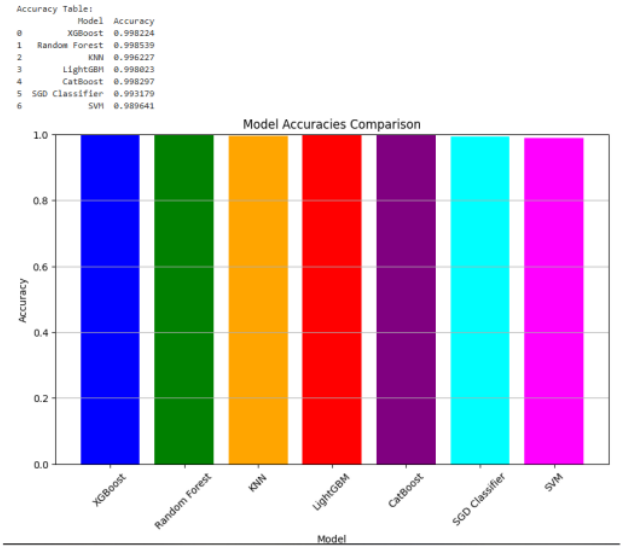
Gambar 3 Grafik Perbandingan Antar Model Pada 6 Kategori

3.3 Hasil pengujian Penyerangan Siber yang dibagi menjadi 2 kategori

Berdasarkan eksperimen yang bertujuan untuk mengevaluasi kinerja berbagai model pembelajaran mesin dalam mendeteksi serangan pada jaringan Internet of Medical Things (IoMT) yang dibagi menjadi 2 ketegori sesuai dengan tabel 1 diatas. Model yang diuji termasuk XGBoost, Random Forest, K-Nearest Neighbors (KNN), LightGBM, CatBoost, SGD Classifier, dan Support Vector Machine (SVM). Hasil ditunjukan pada tabel 4 bahwa Random Forest, Catboost, XGBoosts, dan LightGBM memiliki akurasi tertinggi sebesar 99.8 %, diikuti dengan KNN 99.6% sedangkan untuk model SGD Classifier dan SVM memiliki kinerja yaitu 99.3% dan 98.9%.

Table 4 Hasil Perbandingan antar model dalam 2 kategori

Nama Model	Akurasi (%)	Precision	Recall	F1-Score
Random Forest	99.8	0.99	0.98	0.98
CatBoost	99.8	0.98	0.98	0.98
XGBoost	99.8	0.98	0.98	0.98
LightGBM	99.8	0.98	0.98	0.98
KNN	99.6	0.97	0.95	0.96
SGD Classifier	99.3	0.93	0.91	0.92
SVM	98.9	0.87	0.92	0.89



Gambar 4 Grafik Perbandingan Antar Model Pada 2 Kategori

4. KESIMPULAN

Pada hasil eksperimen dari ketiga model diatas menunjukkan bahwa model terbaik untuk mendeteksi serangan pada IoMT adalah Random Forest, XGBoost, dan CatBoost, dengan akurasi di atas 99%. Namun, performanya komputasi yang lebih tinggi dan kelemahan model seperti KNN, SVM, dan SGD Classifier dalam menangani dataset yang kompleks tetap ada.

Penanganan ketidakseimbangan data, eksplorasi deep learning (LSTM, Autoencoders), dan optimasi hyperparameter dapat meningkatkan penelitian ke depan. Untuk memastikan efektivitas model secara real-time, juga diperlukan uji coba dalam lingkungan nyata.

REFERENSI

[1] 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.

[2] 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.

[3] 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.

[4] BSSN, "Lanskap Keamanan Siber Indonesia," 2024. [Daring]. Tersedia pada: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[5] 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.

[6] 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.

[7] N. Moustafa, B. Turnbull, dan K. K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things," *IEEE Internet Things J.*, vol. 6, no. 3, 2019, doi: 10.1109/JIOT.2018.2871719.

[8] 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.

[9] S. Dadkhah, "CICIoMT 2024," University of New Brunswick. Diakses: 14 Oktober 2024. [Daring]. Tersedia pada: https://www.unb.ca/cic/datasets/iomt-dataset-2024.html

[10] 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.

[11] M. Narang, A. Jatain, dan N. Punetha, "A study on Cyber-attack detection in IoMT using Machine Learning Techniques," *SSRN Electron. J.*, 2023, doi: 10.2139/ssrn.4387775.

[12] 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

[13] 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.

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

[15] D. Faisal, M. Reza ; T. Nugrahadi, *Belajar Data Science: Klasifikasi dengan Bahasa Pemrograman R*, no. February. 2016.

Jurnal InComTech April 2025-Roymond Chandra P.docx

ORIGINALITY REPORT

22%	16%	7%	13%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Institut Teknologi Kalimantan Student Paper	7%
2	jurnal.upnyk.ac.id Internet Source	3%
3	Submitted to University of Westminster Student Paper	1%
4	123dok.com Internet Source	1%
5	Submitted to Universitas Maritim Raja Ali Haji Student Paper	1%
6	Submitted to Coventry University Student Paper	1%
7	Ahmed Shebl, E. I. Elsedimy, A. Ismail, A.A. Salama, Mostafa Herajy. "DCNN: a novel binary and multi-class network intrusion detection model via deep convolutional neural network", EURASIP Journal on Information Security, 2024 Publication	1%

8	publikasi.mercubuana.ac.id Internet Source	1 %
9	rgu-repository.worktribe.com Internet Source	1 %
10	Yanuarini Nur Sukmaningtyas, Ronny Makhfuddin Akbar, Gita Rohma Utami Asyafiiyah. "Penerapan Predictive Analytics untuk Analisis Faktor-faktor yang Mempengaruhi Performa Akademik Siswa", Arcitech: Journal of Computer Science and Artificial Intelligence, 2024 Publication	1 %
11	Dyan Prawita Sari, Zuhri Halim, Irlon Irlon, Bayu Waseso, Saromah Saromah. "Implementasi Machine Learning untuk Deteksi Intrusi pada Jaringan Komputer", Jurnal Minfo Polgan, 2024 Publication	<1 %
12	cyberthreat.id Internet Source	<1 %
13	Wilianto Wilianto, Yuliana Yuliana, Albert Suwandhi, Jimmy Jimmy, Jati Putra. "Penerapan AI dalam Menentukan Harga Mobil Bekas Berdasarkan Tahun Perakitan", Jurnal Minfo Polgan, 2024 Publication	<1 %
	studenttheses.uu.nl	

14	Internet Source	<1%
15	Hamzeh Jehad, Mwaffaq Abu Alhija, Hassan Tarawneh. "" Evaluating the Impact of Adaptive External Dictionaries on Cyberbullying Detection using Machine Learning: A Review"", Research Square Platform LLC, 2023 Publication	<1%
16	Mallikarjun Anandhalli, Vishwanath P. Baligar. "Vehicle Detection and Tracking Based on Color Feature", 2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT), 2017 Publication	<1%
17	jurnal.polinela.ac.id Internet Source	<1%
18	medium.com Internet Source	<1%
19	ojs.uho.ac.id Internet Source	<1%
20	www.researchgate.net Internet Source	<1%
21	databoks.katadata.co.id Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		