JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 5, No. 1, Januari 2026, pp. 71 - 83
p-ISSN : 2803-1507 (media cetak) | e-ISSN : 2803-1531 (media online)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/169

A Systematic Literature Review of Artificial Intelligence-Based Anomaly Detection for Network Intrusion in IoT

Mirza Putra Firmansyah*[1], Muhammad Naufal Nashir[2], Nazli Rahmeisi[3], Putri Safira Augusta[4], Arief Arfriandi[5]
[1,2,3,4,5] Fakultas Teknik, Universitas Negeri Semarang
Jl. Sekaran, Gunungpati, 50229, Kota Semarang, Jawa Tengah, Indonesia
e-mail: mirzafirmansyah66@students.unnes.ac.id*[1], mnnashir083@students.unnes.ac.id[2], nazlirahmeisi@students.unnes.ac.id[3], safiraaugusta83@students.unnes.ac.id[4], arfriandi@mail.unnes.ac.id[5]

ARTICLE INFO

Article History:

Received: 11-10-2025
Revised: 04-11-2025
Accepted: 06-12-2025
Published: 21-01-2026

ABSTRACT

The exponential growth of the Internet of Things (IoT) has created significant network security challenges, particularly in the face of network intrusions, where traditional detection methods often fail against adaptive attacks. This study presents a PRISMA-guided Systematic Literature Review (SLR) to understand the use of Artificial Intelligence (AI) in anomaly detection in IoT. The objectives are to identify dominant AI algorithms, evaluate their performance, and assess energy-efficiency considerations in recent research. The SLR analyzed 24 primary studies from the Scopus database published between 2021 and 2025. Key findings show the dominance of deep learning algorithms: Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), and hybrid/ensemble models. These approaches have proven to be highly effective, with detection accuracy often exceeding 99% on benchmark datasets. In addition, resource efficiency was identified as a central issue. The solutions implemented included lightweight model optimization, Quantized Autoencoder (QAE) compression, and feature selection, which significantly reduced energy consumption and computational load. This research provides a comprehensive overview of state-of-the-art AI-based IoT anomaly detection, emphasizing the need to balance high accuracy and resource efficiency. As a result, future research should prioritize real-world testing, integrate Explainable AI (XAI), and develop standardized efficiency metrics for more practical and reliable IoT security solutions.

Keywords: *Artificial Intelligence, Anomaly Detection, Network Intrusion, Systematic Literature Review.*

Abstrak

Pertumbuhan eksponensial *Internet of Things* (IoT) menghasilkan tantangan keamanan jaringan yang signifikan, terutama intrusi jaringan, di mana metode deteksi tradisional gagal melawan serangan adaptif. Kajian ini menyajikan *Systematic Literature Review* (SLR) berpedoman PRISMA untuk memahami pemanfaatan *Artificial Intelligence* (AI) dalam deteksi anomali pada IoT. Tujuannya adalah mengidentifikasi algoritma AI yang dominan, mengevaluasi performa, dan menilai pertimbangan efisiensi energi dalam penelitian terkini. SLR menganalisis 24 studi primer dari basis data Scopus yang diterbitkan antara tahun

DOI: https://doi.org/10.51903/eqne0j35

p-ISSN : 2803-1507 e-ISSN : 2803-1531

2021 hingga 2025. Temuan utama menunjukkan dominasi algoritma *deep learning*: *Convolutional Neural Network* (CNN), *Long Short-Term Memory* (LSTM), dan model hibrida/ensemble. Pendekatan ini terbukti sangat efektif, dengan akurasi deteksi seringkali melebihi 99% pada *dataset benchmark*. Selain itu, efisiensi sumber daya diidentifikasi sebagai isu sentral. Solusi yang diimplementasikan meliputi optimalisasi model ringan, kompresi *Quantized Autoencoder* (QAE), dan seleksi fitur, yang secara signifikan mengurangi konsumsi energi dan beban komputasi. Penelitian ini memberikan gambaran komprehensif mengenai *state-of-the-art* deteksi anomali IoT berbasis AI, menegaskan perlunya keseimbangan antara akurasi tinggi dan efisiensi sumber daya. Implikasinya, riset mendatang disarankan untuk memprioritaskan pengujian di dunia nyata, mengintegrasikan *Explainable AI* (XAI), dan mengembangkan metrik efisiensi yang terstandarisasi demi solusi keamanan IoT yang lebih praktis dan terpercaya.

Kata Kunci: *Artificial Intelligence, Deteksi Anomali, Intrusi Jaringan, Internet of Things, Systematic Literature Review.*

1. PENDAHULUAN

Perkembangan *Internet of Things* (*IoT*) telah mendorong transformasi besar dalam berbagai sektor, mulai dari industri manufaktur, kesehatan, transportasi, hingga sistem rumah pintar [1], [2], [3]. *IoT* memungkinkan berbagai perangkat fisik untuk saling terhubung melalui jaringan internet, mendukung otomatisasi dan pengambilan keputusan secara *real-time*. Namun, pertumbuhan eksponensial ini juga menghadirkan tantangan serius terkait keamanan jaringan. Setiap perangkat *IoT* yang terhubung berpotensi menjadi titik masuk bagi serangan siber (*cyberattack*), termasuk *network intrusion* yang dapat menimbulkan dampak signifikan baik dari sisi ekonomi maupun operasional [4]. Kondisi ini menjadikan isu keamanan pada *IoT networks* sebagai salah satu fokus utama penelitian di bidang sistem informasi dan keamanan jaringan [5].

Fenomena serangan siber terhadap jaringan *IoT* terus meningkat dari tahun ke tahun. Menurut laporan *Threat Intelligence* tahun 2024, serangan *Distributed Denial of Service* (*DDoS*) yang memanfaatkan botnet *IoT* meningkat hingga lima kali lipat dalam satu tahun terakhir [6]. Salah satu bentuk serangan yang paling dominan adalah *network intrusion*, yang mencakup berbagai upaya eksploitasi celah keamanan perangkat *IoT*. Studi terbaru menunjukkan bahwa metode deteksi berbasis aturan (*signature-based detection*) semakin kurang efektif dalam menghadapi pola serangan baru yang lebih kompleks dan adaptif [7]. Pada kasus serangan *botnet* terhadap perangkat *IoT*, misalnya, banyak sistem konvensional gagal mendeteksi anomali secara akurat karena pola lalu lintas yang sangat dinamis dan heterogen [8]. Hal ini menuntut pendekatan deteksi intrusi yang lebih cerdas, adaptif, dan mampu mengenali pola anomali yang tidak terdefinisi sebelumnya.

Dalam konteks tersebut, *Artificial Intelligence* (AI) mulai banyak diadopsi sebagai solusi alternatif dalam pengembangan sistem deteksi intrusi berbasis anomali. Berbagai pendekatan seperti *Machine Learning* dan *Deep Learning* menawarkan kemampuan untuk menganalisis lalu lintas jaringan, mengenali serangan yang belum pernah terdokumentasi (*zero-day*), serta menyesuaikan model deteksi dengan perubahan pola ancaman [8], [9]. Keunggulan ini menjadikan AI sebagai pendekatan yang lebih potensial dibandingkan metode tradisional seperti *signature-based detection*, terutama dalam menghadapi ancaman dinamis dan kompleks [10], [11]. Meski demikian, sejumlah tantangan masih perlu diatasi, di antaranya pemilihan algoritma yang paling sesuai, tingkat performa yang konsisten dalam berbagai skenario serangan, serta keterbatasan sumber daya perangkat IoT yang menuntut efisiensi energi dan memori [12].

Sehubungan dengan itu, kajian ini menyajikan sebuah Systematic Literature Review (SLR) yang difokuskan pada penerapan AI dalam anomaly detection terhadap intrusion pada IoT. Untuk mencapai tujuan tersebut, kajian ini disusun dengan mengacu pada metode Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) dan menggunakan analisis terhadap publikasi terbaru yang terindeks Scopus. Dengan pendekatan ini, diharapkan dapat diperoleh pemahaman yang lebih terstruktur mengenai algoritma AI yang dominan digunakan, kinerja yang dihasilkan, serta sejauh mana isu efisiensi energi telah dipertimbangkan dalam penelitian terkini. Peninjauan tersebut juga memungkinkan pemetaan kecenderungan penelitian yang muncul dalam beberapa tahun terakhir berdasarkan karakteristik metode yang digunakan.

Kebaruan dari penelitian ini terletak pada fokus eksplisit terhadap aspek *energy efficiency* dalam sistem deteksi intrusi berbasis AI untuk IoT—sebuah dimensi yang jarang disoroti secara mendalam dalam SLR sebelumnya. Sebagian besar studi terdahulu, seperti yang dilakukan oleh [6], lebih menitikberatkan pada identifikasi dan evaluasi teknik deteksi terhadap serangan *IoT botnet DDoS* tanpa mempertimbangkan

p-ISSN : 2803-1507 e-ISSN : 2803-1531

efisiensi energi atau keterbatasan perangkat IoT. Demikian pula, [9] menegaskan bahwa penelitian terkait *Intrusion Detection Systems* untuk IoT umumnya menghadapi *trade-off* antara akurasi, konsumsi energi, dan privasi, namun belum banyak kajian yang secara sistematis menelaah isu efisiensi energi sebagai fokus utama. Perhatian terhadap aspek ini semakin relevan mengingat keterbatasan daya pada perangkat IoT yang memerlukan mekanisme deteksi dengan konsumsi energi yang lebih hemat.

2. METODOLOGI PENELITIAN

Dalam kajian ini, kerangka PRISMA digunakan sebagai pedoman utama untuk menyusun systematic literature review. Pendekatan ini dipilih karena mampu memastikan proses pencarian, seleksi, dan evaluasi literatur berlangsung secara sistematis serta transparan [13]. Dengan demikian, analisis terhadap hubungan kecerdasan buatan (AI), network intrusion, dan Internet of Things (IoT) dapat dilakukan secara lebih terstruktur. Hasil dari penerapan metode ini diharapkan menghasilkan temuan yang andal sekaligus memberikan kontribusi ilmiah yang relevan pada bidang yang tengah berkembang pesat tersebut.

2.1. *Research Question Definition*

Dalam penelitian ini, penentuan Research Questions (RQ) didasarkan pada tujuan utama kajian, yaitu untuk memahami pemanfaatan algoritma *Artificial Intelligence* (AI) dalam mendeteksi *anomaly* pada *intrusion* di lingkungan *Internet of Things* (IoT). Pendekatan tersebut memberikan kerangka yang jelas bagi proses identifikasi fokus penelitian dalam domain *cybersecurity*. Penetapan RQ juga memastikan bahwa batasan kajian dapat dipahami secara konsisten sepanjang proses penyusunan *systematic review*. Perumusan RQ mengikuti prinsip yang umum digunakan dalam studi *Systematic Literature Review* (SLR), yakni RQ harus mampu:

1. menggambarkan tren penelitian terkini,
2. mengevaluasi efektivitas pendekatan yang digunakan, serta
3. mengidentifikasi keterbatasan atau faktor yang sering diabaikan dalam penerapan nyata.

Perumusan ini dilakukan setelah berbagai aspek metodologis dianalisis untuk memastikan bahwa fokus penelitian sesuai dengan ruang lingkup kajian. Setiap pertanyaan riset dirancang agar mampu menangkap variasi konsep dan temuan yang muncul dalam literatur terkait integrasi AI pada ekosistem IoT. Struktur ini juga memberikan kejelasan dalam tahapan identifikasi studi primer yang relevan untuk dianalisis. Berdasarkan kerangka tersebut, tiga pertanyaan riset diformulasikan sebagai berikut:

RQ1: Algoritma AI apa yang paling sering digunakan untuk anomaly detection pada intrusion di IoT?

Pertanyaan ini ditujukan untuk mengidentifikasi kecenderungan algoritma yang dominan digunakan oleh peneliti, sehingga dapat memberikan gambaran perkembangan metodologi yang populer dalam bidang ini. Analisis ini memungkinkan peneliti memahami bagaimana preferensi penggunaan algoritma berkembang dari waktu ke waktu. Informasi tersebut juga membantu mengungkap kecocokan algoritma tertentu terhadap karakteristik data dalam ekosistem IoT. Pemahaman mengenai kecenderungan tersebut memberikan konteks yang lebih luas untuk interpretasi hasil penelitian.

RQ2: Seberapa baik performa dari Algoritma AI yang digunakan dalam mendeteksi intrusion di IoT?

RQ ini difokuskan pada evaluasi performa, misalnya melalui metrik akurasi, *precision*, *recall*, F1-score, atau metrik lain yang digunakan dalam studi primer, guna mengetahui sejauh mana efektivitas metode yang diusulkan. Pendekatan ini memungkinkan identifikasi kelebihan dan kekurangan dari teknik yang diterapkan dalam berbagai skenario. Evaluasi performa juga membantu menilai stabilitas algoritma ketika dihadapkan pada variasi data yang kompleks. Pemahaman ini memberi gambaran tentang tingkat reliabilitas metode dalam situasi operasional yang berbeda.

RQ3: Sejauh mana penelitian mempertimbangkan penggunaan energi pada perangkat IoT saat mengimplementasikan AI untuk anomaly detection?

Pertanyaan ini berfungsi untuk menilai apakah penelitian-penelitian terdahulu sudah mengintegrasikan faktor efisiensi energi, mengingat perangkat IoT umumnya memiliki keterbatasan daya dan sumber energi. Penilaian ini penting karena implementasi algoritma yang kompleks dapat meningkatkan konsumsi energi secara signifikan. Banyak perangkat IoT beroperasi dalam kondisi sumber daya terbatas sehingga optimasi energi menjadi aspek kritis. Analisis ini juga membantu memahami bagaimana keseimbangan antara akurasi deteksi dan kebutuhan energi dikelola dalam penelitian sebelumnya.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Penetapan RQ tersebut memberikan struktur analitis yang membantu mengarahkan fokus penelitian pada aspek-aspek yang paling relevan. Setiap RQ berperan dalam memetakan temuan yang muncul dari berbagai studi yang meneliti integrasi AI pada perangkat IoT. Kerangka ini juga mendukung proses evaluasi literatur agar aspek teknis dan non-teknis dapat dianalisis secara seimbang. Dengan menetapkan tiga RQ tersebut, penelitian ini diharapkan mampu memberikan gambaran menyeluruh mengenai: (i) tren algoritma AI yang digunakan, (ii) performa yang dicapai oleh berbagai pendekatan, serta (iii) sejauh mana aspek keberlanjutan dan efisiensi energi diperhatikan dalam konteks *anomaly detection* pada *intrusion* di IoT.

2.2. *Eligibility Criteria*

Untuk menjamin kualitas serta relevansi literatur yang ditelaah, ditetapkan sejumlah kriteria kelayakan yang ketat. Kriteria inklusi difokuskan pada publikasi akademik terkini yang secara spesifik membahas penerapan AI untuk anomaly detection pada network intrusion dalam konteks IoT. Artikel yang dipertimbangkan harus memenuhi beberapa syarat, yaitu diterbitkan dalam lima tahun terakhir (2021–2025), ditulis dalam bahasa Inggris, tersedia dalam bentuk teks lengkap, serta dipublikasikan di jurnal terindeks. Dengan kriteria tersebut, diharapkan cakupan kajian mampu menghadirkan gambaran yang komprehensif sekaligus mutakhir mengenai perkembangan penelitian dalam bidang ini. Selain itu, setiap studi yang dipilih wajib menunjukkan fokus yang jelas pada penerapan AI untuk anomaly detection.

Sementara itu, proses eksklusi dilakukan secara bertahap untuk memastikan literatur yang tersisa benar-benar relevan. Pada tahap awal, artikel yang tidak menyediakan akses teks lengkap dieliminasi karena keterbatasan tersebut akan menghambat evaluasi metodologis maupun hasil penelitian. Tahap berikutnya menyingkirkan studi sekunder, seperti review atau survey, sehingga hanya studi primer yang menjadi perhatian. Terakhir, dilakukan penilaian kualitatif berdasarkan relevansi tematik dan ketelitian metodologis, mencakup evaluasi judul, abstrak, hingga isi teks penuh. Studi yang lolos pada tahap ini adalah studi yang secara langsung berkaitan dengan pertanyaan riset RQ yang telah ditetapkan.

2.3. *Search Strategies and Selection Process*

Proses literature review menggunakan kata kunci untuk menemukan artikel yang relevan dengan topik penelitian. Istilah pencarian dipilih secara hati-hati agar cakupan pencarian dalam Systematic Literature Review (SLR) tetap luas namun tetap fokus pada tema penelitian [14]. Pencarian literatur dilakukan secara sistematis dengan memanfaatkan seperangkat kata kunci yang telah ditentukan sejak tahap awal seleksi. Untuk memperluas cakupan, kata kunci dikombinasikan dalam berbagai bentuk. Istilah terkait Internet of Things (IoT) dipadukan dengan istilah Intrusion Detection atau Network Intrusion, serta dengan istilah Anomaly Detection atau Anomaly Based. Selanjutnya, istilah tersebut juga digabungkan dengan Artificial Intelligence (AI) baik dalam bentuk singkatan maupun penulisan lengkap, serta ditambahkan dengan istilah evaluasi kinerja seperti Performance, Accuracy, atau Efficiency. Pencarian dilakukan pada judul, abstrak, dan kata kunci di basis data Scopus.

Penyusunan kata kunci dilakukan dengan mempertimbangkan hubungan antaristilah yang sering muncul dalam penelitian terkait topik tersebut. Setiap istilah digabungkan melalui operator logis agar pencarian mampu menjangkau publikasi yang memiliki kedekatan tematik. Pendekatan ini digunakan untuk memastikan bahwa struktur pencarian tetap sistematis dan mampu memfokuskan hasil pada penelitian yang relevan. Kombinasi ini menghasilkan kueri pencarian berikut:

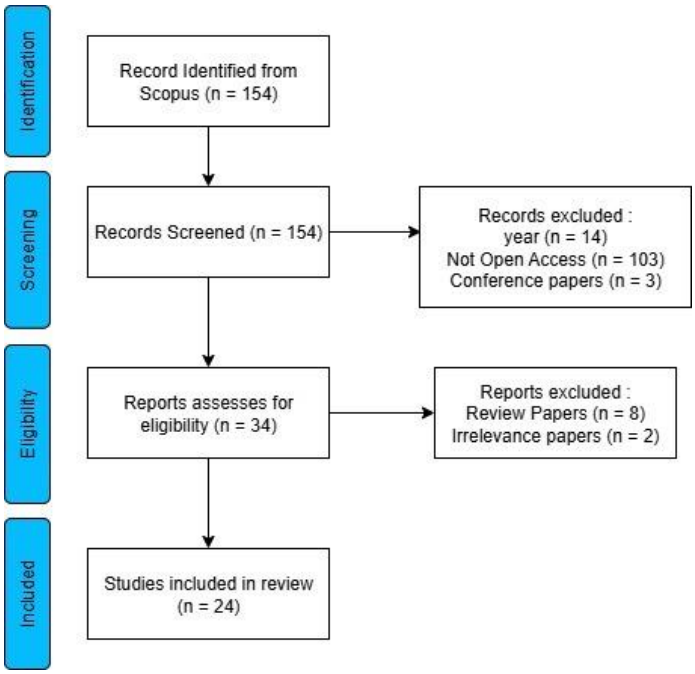
TITLE-ABS-KEY (("Internet of Things" OR "IoT") AND ("Intrusion detection" OR "Network Intrusion") AND ("Anomaly Detection" OR "Anomaly Based") AND ("Artificial Intelligence" OR AI) AND ("Performance" OR "Accuracy" OR "Efficiency"))

Artikel yang diperoleh dari hasil pencarian selanjutnya diseleksi melalui tiga tahap penyaringan. Tahap pertama adalah eliminasi artikel yang tidak menyediakan akses teks lengkap, karena keterbatasan tersebut dapat menghambat proses evaluasi terhadap metodologi maupun hasil penelitian. Tahap kedua berfokus pada penyisihan studi sekunder, seperti *review* atau *survey*, sehingga kajian ini hanya mencakup studi primer yang relevan. Tahap ketiga berupa penilaian kualitatif yang menekankan pada relevansi tematik dan ketelitian metodologis, mencakup evaluasi judul, abstrak, hingga isi teks penuh. Hanya studi yang secara langsung terkait dengan pertanyaan riset (RQ) yang telah ditetapkan yang dipertahankan pada tahap akhir seleksi.

Setiap tahap proses seleksi didokumentasikan sesuai dengan pedoman PRISMA, dengan pencatatan sistematis mengenai jumlah studi yang teridentifikasi, dieliminasi, dan akhirnya disertakan dalam kajian.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Penerapan prosedur yang ketat ini bertujuan untuk menjamin tingkat transparansi dan reprodusibilitas penelitian. Ringkasan proses seleksi tersebut kemudian divisualisasikan dalam bentuk diagram alir PRISMA seperti yang ditunjukkan pada Gambar 1, yang menggambarkan alur mulai dari tahap identifikasi awal hingga inklusi akhir studi.



Gambar 1. Diagram alir PRISMA

2.4. *Data Extraction and Synthesis*

Data yang relevan diekstraksi dari 24 studi primer yang dipilih untuk menjawab tiga Research Questions (RQ) yang telah ditetapkan. Setiap artikel ditinjau secara menyeluruh guna mengumpulkan informasi yang berkaitan langsung dengan fokus penelitian. Proses ekstraksi diarahkan untuk memperoleh data mengenai identifikasi algoritma AI yang digunakan (RQ1), evaluasi performa algoritma dalam mendeteksi intrusion pada IoT (RQ2), serta sejauh mana pertimbangan efisiensi energi diperhatikan dalam implementasinya (RQ3). Ekstraksi data dilakukan oleh penulis pertama dan kedua, kemudian hasilnya ditinjau serta diverifikasi oleh penulis ketiga dan keempat. Setiap perbedaan temuan atau konflik selama proses ekstraksi diselesaikan melalui diskusi bersama hingga tercapai kesepakatan.

Setelah proses ekstraksi selesai, tahap berikutnya adalah sintesis data. Pada tahap ini, data yang telah terkumpul dianalisis dan diinterpretasikan untuk menghasilkan wawasan yang selaras dengan ketiga pertanyaan penelitian. Baik data kualitatif maupun kuantitatif dipertimbangkan untuk memberikan gambaran yang komprehensif. Hasil ekstraksi kemudian diringkas dan dipaparkan secara sistematis sehingga tetap ringkas namun cukup jelas untuk dipahami oleh pembaca. Dengan demikian, proses sintesis tidak hanya menyoroti temuan utama dari studi primer, tetapi juga memastikan bahwa informasi penting tidak terlewatkan maupun disalahartikan.

3. HASIL DAN PEMBAHASAN

3.1. *Klasifikasi Algoritma AI untuk Deteksi Anomali IOT*

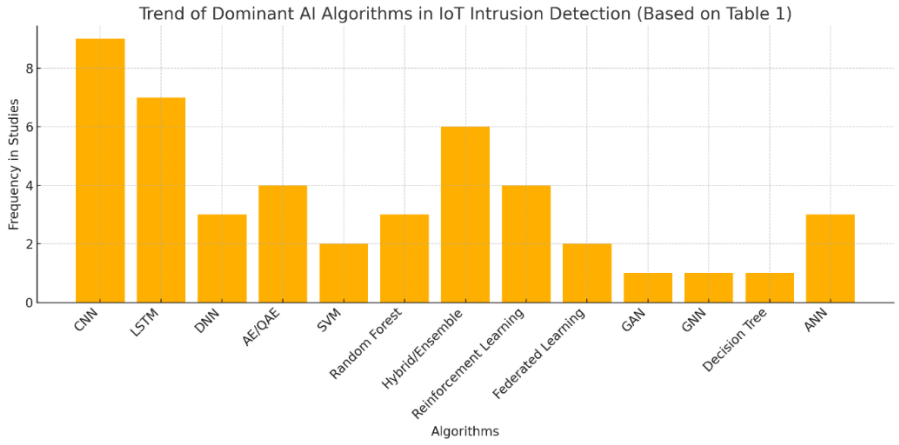
Berdasarkan hasil analisis terhadap 24 artikel yang dikaji, penerapan kecerdasan buatan dalam sistem deteksi anomali IoT mencakup beragam jenis algoritma dengan karakteristik dan peran yang berbeda. Seperti ditunjukkan pada Tabel 1, serta divisualisasikan pada Gambar 2, terdapat tiga pendekatan utama yang paling dominan digunakan, yaitu Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), dan model hibrida/ensemble. Ketiga pendekatan ini mendominasi karena menawarkan kemampuan komplementer dalam proses deteksi. Sumber-sumber tersebut menunjukkan variasi pendekatan dalam

p-ISSN : 2803-1507 e-ISSN : 2803-1531

memanfaatkan algoritma kecerdasan buatan sehingga analisis komparatif diperlukan untuk memahami keunggulan masing-masing metode pada konteks *Internet of Things*.

Tabel 1. Klasifikasi Algoritma AI

Algoritma AI	Frekuensi	Studi yang dikaji
Convolutional Neural Network (CNN)	9	[15], [16], [17], [18], [19], [20], [21], [22], [23]
Long Short-Term Memory (LSTM)	7	[15], [16], [24], [18], [19], [21], [25]
Deep Neural Network (DNN)	3	[26], [27], [23]
Autoencoder (AE) / Quantized AE	4	[28], [29], [30], [31]
Support Vector Machine (SVM)	2	[29], [32]
Random Forest (RF)	3	[17], [28], [33]
Model Hibrida / Ensemble (CNN–LSTM, AE–CatBoost, Transformer, DNN-CSO)	6	[17], [26], [24], [34], [18], [19]
Reinforcement Learning (RL)	4	[34], [22], [35], [36]
Federated Learning (FL)	2	[18], [27]
Generative Adversarial Network (GAN)	1	[29]
Graph Neural Network (GNN)	1	[22]
Decision Tree (DT)	1	[37]
Artificial Neural Network (ANN)	3	[38], [31], [20]



Gambar 2. Tren Dominan AI pada IoT

Algoritma CNN digunakan secara luas berkat kemampuannya dalam mengenali pola dan fitur spasial dari lalu lintas jaringan. Kekuatan ini menjadikannya sangat efektif dalam mendeteksi serangan seperti DDoS atau penyusupan berbasis pola. Namun, CNN juga memiliki beberapa kelemahan yang penting diperhatikan. Proses konvolusi pada CNN bersifat komputasi-intensif, sehingga memerlukan daya pemrosesan tinggi dan konsumsi energi yang tidak sedikit. Kondisi ini dapat menjadi kendala ketika diterapkan pada perangkat IoT berdaya rendah yang memiliki keterbatasan CPU dan memori. Selain itu, CNN kurang optimal dalam menangani pola temporal yang bergantung pada urutan waktu, sehingga sering kali memerlukan integrasi dengan model sekuensial seperti LSTM.

Sementara itu, LSTM unggul dalam mempelajari pola temporal secara mendalam, sehingga cocok untuk mendeteksi anomali jaringan yang muncul secara berurutan. Keunggulan ini menjadikan LSTM efektif dalam lingkungan IoT yang menghasilkan data kontinu. Namun, model LSTM memiliki arsitektur internal yang lebih kompleks dibandingkan CNN, sehingga memerlukan komputasi dan memori yang lebih besar. Hal ini dapat meningkatkan latensi, terutama jika model dijalankan langsung pada perangkat edge. Dengan demikian, meskipun LSTM memberikan performa deteksi yang sangat baik, implementasinya membutuhkan optimasi tambahan agar efisien pada perangkat IoT terbatas.

Model hibrida dan ensemble muncul sebagai pendekatan yang menggabungkan kelebihan dari berbagai algoritma. Misalnya, CNN–LSTM mampu menangkap fitur spasial sekaligus temporal, sementara kombinasi seperti CatBoost–XGBoost–LightGBM memaksimalkan kekuatan masing-masing algoritma berbasis boosting. Meskipun menawarkan akurasi tertinggi, model hibrida memiliki kompleksitas yang lebih besar, sehingga berpotensi meningkatkan waktu pelatihan, konsumsi energi, dan kebutuhan memori. Dengan

p-ISSN : 2803-1507 e-ISSN : 2803-1531

demikian, terdapat trade-off antara performa tinggi dan efisiensi sumber daya yang harus dipertimbangkan ketika mengimplementasikannya pada IoT skala besar.

Secara keseluruhan, hasil klasifikasi algoritma AI pada penelitian ini menunjukkan bahwa CNN, LSTM, dan model hibrida/ensemble menjadi pendekatan dominan yang digunakan dalam deteksi anomali IoT. Ketiganya menawarkan mekanisme yang saling melengkapi: CNN unggul dalam ekstraksi fitur spasial, LSTM efektif dalam pemodelan data sekuensial, dan model hibrida/ensemble mampu meningkatkan performa deteksi dengan mengombinasikan keunggulan dari berbagai algoritma. Keberagaman pendekatan ini mencerminkan bagaimana algoritma AI berkontribusi dalam memperkuat sistem keamanan IoT agar lebih cerdas, efisien, dan tangguh terhadap serangan siber yang semakin kompleks. Keragaman ini memberikan dasar bagi pengembangan strategi deteksi yang lebih adaptif sehingga mekanisme identifikasi anomali dapat disesuaikan dengan kebutuhan operasional pada lingkungan *Internet of Things*.

3.2. *Performa Algoritma AI pada Deteksi Anomali IOT*

Analisis pada bagian ini menyintesis temuan-temuan kuantitatif dari literatur yang dikaji untuk menjawab pertanyaan penelitian mengenai efektivitas algoritma AI dalam mendeteksi intrusi di lingkungan IoT. Evaluasi ini difokuskan pada metrik akurasi yang dilaporkan oleh penelitian-penelitian primer. Pendekatan analitis ini memberikan gambaran yang lebih rinci mengenai bagaimana parameter evaluasi diterapkan pada berbagai skenario pengujian. Mekanisme pengukuran tersebut membantu menjelaskan konteks penggunaan metrik akurasi dalam studi-studi terdahulu.

Convolutional Neural Network (CNN) menunjukkan kinerja yang menjanjikan dalam mendeteksi anomali jaringan IoT berkat kemampuannya dalam ekstraksi fitur secara otomatis dari data mentah [21], [23]. Sebelum membahas hasil performa secara spesifik, penting untuk memahami bagaimana metrik tersebut diperoleh. Dalam artikel-artikel yang dikaji, performa model AI dievaluasi melalui serangkaian eksperimen yang menggunakan *dataset benchmark* standar di bidang keamanan siber [17]. *Dataset* ini, yang berisi kumpulan lalu lintas jaringan normal maupun berbagai jenis serangan, menjadi dasar untuk melatih dan menguji model secara objektif.

Para peneliti umumnya menggunakan dataset seperti NSL-KDD, UNSW-NB15, CIC-IDS2017, dan BoT-IoT [15], [16], [22]. Proses evaluasi ini melibatkan pembagian dataset menjadi data latih (training set) dan data uji (testing set). Dengan membandingkan prediksi model dengan label sebenarnya pada data uji, tingkat akurasi dapat dihitung untuk mengukur efektivitas CNN dalam mengidentifikasi intrusi [17], [18], [19]. Pendekatan ini memastikan bahwa performa akurasi yang dilaporkan bersifat objektif dan dapat diperbandingkan. Ringkasan akurasi berbagai model yang dikaji dapat dilihat pada Tabel 2, yang merangkum performa beberapa algoritma AI berdasarkan dataset dan arsitektur yang digunakan.

Tabel 2. Perbandingan performa Algoritma AI

Algoritma	Dataset	Deskripsi	Akurasi
CNN–LSTM (hibrida)	Beberapa dataset IoT	Kombinasi CNN untuk ekstraksi fitur + LSTM untuk analisis temporal	99.81%
Multi-Deep Learning (CNN dalam kerangka multi-DL)	Kitsune	Digunakan untuk deteksi anomali IoT berbasis autoencoder	99.83%
Multi-Deep Learning (CNN dalam kerangka multi-DL)	5G-NIDD	Digunakan untuk deteksi anomali pada sistem 5G	99.27%
LSTM–FL (Federated Learning)	UNSW-NB15	Arsitektur terdesentralisasi, cocok untuk IoT	99.17%
LSTM–FL (Federated Learning)	CIC-IDS2017	Model yang sama tetapi diuji dataset berbeda	99.94%
Optimized Lightweight LSTM	IoT-23	LSTM dioptimasi untuk perangkat IoT resource-limited	94.78% (naik dari 94.2%)
K-Means + Random Forest (hibrida)	CIC-IDS2017	Pendekatan hierarkis: unsupervised + supervised	99.5%
CatBoost + XGBoost + LightGBM (ensemble)	KDDCUP 99	Boosting-based ensemble dengan seleksi fitur	99.95%
CatBoost + XGBoost + LightGBM (ensemble)	UNSW-NB15	Dataset yang sama, performa lebih rendah	97.47%

Dalam hal akurasi, penelitian yang dikaji menunjukkan bahwa model berbasis CNN mampu mencapai tingkat keberhasilan yang sangat tinggi. Kemampuannya untuk mengekstraksi fitur relevan secara otomatis menjadi faktor kunci. Sebagai contoh, model hibrida yang menggabungkan CNN dengan LSTM berhasil mencapai akurasi 99.81% pada beberapa *dataset* IoT [15]. Tingginya akurasi juga dilaporkan oleh [20], di mana model AI mereka—yang diuji pada *dataset* UNSW-NB15 dan TON_IoT—menunjukkan kinerja yang sangat baik dalam mendeteksi anomali di lingkungan *Internet of Healthcare Things* (IoHT). Pencapaian tersebut menunjukkan konsistensi kinerja model dalam berbagai kondisi pengujian.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Studi lain yang mengintegrasikan CNN dalam kerangka *multi-deep learning* juga melaporkan tingkat akurasi yang sangat kompetitif, dengan capaian 99.83% pada *dataset* Kitsune dan 99.27% pada *dataset* 5G-NIDD [16]. Fleksibilitas CNN juga terbukti dalam domain spesifik seperti *Cooperative Intelligent Transportation Systems* (C-ITS), di mana model CNN digunakan untuk mengklasifikasikan perilaku anomali dalam komunikasi antar kendaraan [21]. Keberhasilan penerapan di berbagai skenario, mulai dari IoT umum, IoHT, hingga C-ITS, memperkuat posisi CNN sebagai salah satu algoritma yang paling efektif dan andal untuk tugas deteksi intrusi. Penerapan tersebut menunjukkan bahwa arsitektur CNN mampu beradaptasi terhadap variasi pola data yang muncul dalam sistem komunikasi modern.

Selanjutnya, pembahasan beralih ke *Long Short-Term Memory* (LSTM), algoritma yang dirancang khusus untuk mengenali pola temporal dan dependensi jangka panjang dalam data sekuensial [21]. Karakteristik ini menjadikannya sangat relevan untuk analisis lalu lintas jaringan IoT, di mana urutan paket data dari waktu ke waktu dapat mengindikasikan adanya anomali atau serangan. Keunggulan ini tidak hanya terletak pada kemampuannya mendeteksi, tetapi juga potensinya untuk diintegrasikan dalam kerangka kerja yang dapat menjelaskan keputusannya (*explainable AI*), sebuah aspek krusial untuk membangun kepercayaan pada sistem deteksi [25]. Pendekatan tersebut memungkinkan sistem untuk memanfaatkan dinamika waktu sebagai sumber informasi penting dalam proses identifikasi anomali.

Metodologi untuk mengevaluasi kinerja LSTM dalam artikel yang dikaji umumnya melibatkan pengujian pada *dataset benchmark*. Para peneliti memanfaatkan *dataset* publik seperti UNSW-NB15, CIC-IDS2017, dan IoT-23 untuk melatih dan menguji model mereka, memastikan hasil yang dilaporkan dapat diverifikasi dan diperbandingkan [24], [18], [19]. Proses ini melibatkan pembagian *dataset* menjadi data latih dan uji untuk mengukur seberapa akurat model LSTM dapat membedakan aktivitas normal dari anomali pada data yang belum pernah ditemui sebelumnya. Pendekatan evaluasi tersebut memberikan gambaran yang lebih jelas mengenai kemampuan model dalam menghadapi variasi distribusi data pada skenario dunia nyata.

Dari segi akurasi, LSTM menunjukkan kinerja yang sangat andal, terutama saat dioptimalkan atau digabungkan dengan teknologi lain. Sebagai contoh, pada arsitektur hibrida CNN-LSTM, model ini berhasil mencapai akurasi 99.81%, membuktikan bahwa kemampuan analisis sekuensial LSTM dapat bersinergi dengan baik dengan ekstraksi fitur CNN [15]. Dalam implementasi lain yang berfokus pada arsitektur terdesentralisasi, seperti pada kerangka berbasis *Federated Learning* (FL), model LSTM juga menunjukkan performa luar biasa dengan akurasi 99.17% pada *dataset* UNSW-NB15 dan 99.94% pada *dataset* CIC-IDS2017 [18]. Temuan ini menunjukkan bahwa kemampuan LSTM untuk menangkap pola temporal dapat dimanfaatkan secara optimal dalam berbagai konfigurasi desain model.

Fleksibilitas LSTM juga terlihat pada kemampuannya untuk dioptimalkan dalam kerangka keamanan yang ringan (*lightweight*). Sebuah penelitian berhasil meningkatkan akurasi model varian LSTM dari 94.2% menjadi 94.78% pada *dataset* IoT-23 melalui proses optimisasi, yang sangat penting untuk perangkat IoT dengan sumber daya komputasi terbatas [24]. Penerapan efektif di berbagai skenario, termasuk untuk sistem transportasi cerdas (C-ITS) [21], mengonfirmasi bahwa LSTM merupakan algoritma yang serbaguna, mampu memberikan akurasi tinggi baik dalam arsitektur yang kompleks maupun yang efisien. Peningkatan ini menunjukkan bahwa struktur internal LSTM dapat disesuaikan untuk mencapai performa optimal tanpa kebutuhan komputasi yang berlebihan.

Selain penerapan algoritma secara individual, banyak penelitian yang dikaji mengadopsi model hibrida atau *ensemble* untuk meningkatkan performa deteksi. Pendekatan ini didasarkan pada prinsip bahwa penggabungan kekuatan dari beberapa algoritma yang berbeda dapat menutupi kelemahan masing-masing model, sehingga menghasilkan sistem deteksi yang lebih kuat dan akurat. Meskipun kombinasi CNN dan LSTM seperti yang telah dibahas sebelumnya merupakan contoh populer, berbagai bentuk arsitektur hibrida lain juga menunjukkan kinerja yang sangat efektif. Konsep ini memungkinkan setiap komponen algoritma memberikan kontribusi unik yang memperkaya kapasitas deteksi keseluruhan.

Proses evaluasi untuk model hibrida ini tetap mengandalkan pengujian pada *dataset benchmark* standar, seperti KDDCUP 99, UNSW-NB15, dan CIC-IDS2017, untuk memastikan validitas dan komparabilitas hasil [17], [19]. Dengan menggabungkan beberapa teknik, model-model ini diuji kemampuannya untuk mencapai akurasi yang lebih tinggi dibandingkan jika komponennya digunakan secara terpisah. Pengujian tersebut memberikan gambaran menyeluruh mengenai bagaimana kombinasi algoritma berfungsi pada variasi skenario serangan. Pendekatan evaluatif ini juga membantu mengidentifikasi kondisi eksperimental yang paling mendukung peningkatan kinerja model.

Berbagai implementasi menunjukkan keberhasilan pendekatan ini. Sebagai contoh, [19] mengembangkan sistem deteksi hierarkis yang mengintegrasikan klastering K-Means dengan klasifikasi Random Forest. Model ini menunjukkan akurasi sebesar 99.5% pada *dataset* CIC-IDS2017, membuktikan bahwa kombinasi metode *unsupervised* dan *supervised learning* dapat menghasilkan deteksi yang sangat presisi. Sementara itu,

p-ISSN : 2803-1507 e-ISSN : 2803-1531

[17] menerapkan pendekatan *ensemble learning* yang menggabungkan tiga algoritma *boosting* kuat: CatBoost, XGBoost, dan LightGBM. Setelah melalui tahap seleksi fitur yang canggih, model *ensemble* ini berhasil mencapai akurasi 99.95% pada *dataset* KDDCUP 99 dan 97.47% pada *dataset* UNSW-NB15. Contoh-contoh tersebut menunjukkan variasi metode yang dapat dimanfaatkan untuk meningkatkan kualitas deteksi berdasarkan karakteristik dataset yang digunakan.

Pendekatan hibrida tidak hanya terbatas pada penggabungan beberapa pengklasifikasi, tetapi juga kombinasi antara teknik seleksi fitur dan algoritma AI untuk meningkatkan efisiensi dan fokus deteksi [26]. Berbagai contoh ini menunjukkan bahwa model hibrida dan *ensemble* secara konsisten memberikan tingkat akurasi yang sangat tinggi, seringkali melampaui performa model tunggal, menjadikannya strategi yang sangat efektif dalam pengembangan sistem deteksi intrusi IoT modern. Pendekatan seperti ini memungkinkan sistem memanfaatkan informasi yang lebih terstruktur sebelum memasuki tahap klasifikasi. Penggabungan teknik tersebut membantu memperkuat kemampuan model dalam mengenali pola serangan yang kompleks dan beragam.

3.3. *Pertimbangan Efisiensi Energi pada Deteksi Anomali Berbasis AI*

Analisis literatur menunjukkan bahwa keterbatasan sumber daya, terutama konsumsi energi, merupakan pertimbangan krusial dalam implementasi AI untuk deteksi anomali pada perangkat IoT. Penelitian yang dikaji tidak hanya berfokus pada akurasi deteksi, tetapi juga secara aktif mengembangkan berbagai strategi untuk memastikan solusi yang diusulkan bersifat ringan (lightweight) dan efisien secara energi, sehingga layak diterapkan di lingkungan IoT yang seringkali memiliki keterbatasan daya dan komputasi. Upaya ini menggambarkan bahwa penghematan energi harus dipertimbangkan sebagai bagian integral dari perancangan sistem deteksi anomali berbasis AI.

Salah satu pendekatan utama yang diidentifikasi adalah optimalisasi dan pengembangan model AI yang ringan. [24], misalnya, mengusulkan kerangka kerja keamanan yang secara eksplisit dirancang untuk menjadi "ringan" dan cocok untuk lingkungan dengan sumber daya terbatas. Melalui teknik optimalisasi, kerangka kerja ini tidak hanya meningkatkan akurasi tetapi juga berhasil mengoptimalkan konsumsi energi sebesar 12.01%. Sejalan dengan itu, [38] mengembangkan kerangka kerja deteksi intrusi berbasis perangkat keras heterogen yang menggunakan model jaringan saraf tiruan ringan untuk mencapai konsumsi daya sangat rendah (ultra-low power consumption).

Selain optimalisasi, teknik kompresi model juga menjadi solusi efektif untuk mengurangi beban komputasi. [30] memperkenalkan *Quantized Autoencoder* (QAE), sebuah model yang dioptimalkan melalui teknik pruning, clustering, dan kuantisasi integer. Implementasi QAE terbukti secara drastis mengurangi beban komputasi, dengan penurunan pemanfaatan memori rata-rata sebesar 70.01% dan pemanfaatan CPU puncak sebesar 27.94%, yang secara langsung berimplikasi pada penghematan energi signifikan pada perangkat IoT.

Pendekatan lain yang berkontribusi pada efisiensi energi adalah melalui seleksi fitur yang efisien. Dengan mengurangi jumlah fitur yang perlu diproses, beban komputasi pada perangkat dapat diminimalkan. [33] menekankan bahwa seleksi fitur yang efisien sangat penting untuk perangkat IoT yang memiliki keterbatasan daya, memori, dan energi. Metode yang mereka usulkan bertujuan untuk mengurangi dimensi fitur sambil mempertahankan akurasi deteksi yang tinggi, sehingga meningkatkan efisiensi komputasi secara keseluruhan. Terakhir, beberapa penelitian mengatasi masalah energi dari perspektif arsitektur sistem. [27] menyoroti bahwa arsitektur keamanan terpusat tradisional cenderung menyebabkan konsumsi energi yang tinggi. Solusi hibrida mereka yang menggabungkan AI dengan blockchain terbukti mampu menurunkan konsumsi energi hingga 31.8% dibandingkan pendekatan konvensional, memvalidasi efisiensinya untuk jaringan IoT skala besar.

Secara keseluruhan, penelitian-penelitian ini secara tegas menunjukkan bahwa efisiensi energi bukanlah pertimbangan sekunder, melainkan komponen inti dalam desain sistem deteksi anomali berbasis AI untuk IoT. Berbagai inovasi, mulai dari penciptaan model yang ringan, kompresi model, seleksi fitur yang cerdas, hingga desain arsitektur yang terdesentralisasi, secara kolektif menunjukkan kemajuan signifikan dalam mewujudkan solusi keamanan yang tidak hanya akurat tetapi juga hemat daya. Pendekatan tersebut memperlihatkan bahwa setiap tahap pemrosesan dapat diarahkan untuk mengurangi penggunaan energi tanpa mengorbankan kualitas deteksi. Inisiatif ini juga menegaskan bahwa aspek efisiensi energi perlu disinergikan dengan kebutuhan operasional jaringan IoT modern.

4. DISKUSI

Hasil *systematic literature review* ini menunjukkan bahwa penerapan kecerdasan buatan dalam pendidikan terutama berfokus pada personalisasi pembelajaran, suatu temuan yang sejalan dengan penjelasan dalam [3] mengenai peran *adaptive learning* dalam meningkatkan relevansi materi bagi siswa. Analisis terhadap

p-ISSN : 2803-1507 e-ISSN : 2803-1531

sejumlah artikel memperlihatkan bahwa teknologi seperti *learning analytics* membantu mengidentifikasi pola belajar sehingga memungkinkan intervensi yang lebih tepat waktu. Kesesuaian antara tren penelitian ini dengan penjelasan dalam [7] mengindikasikan bahwa pendekatan berbasis data semakin menjadi landasan utama dalam pengembangan metode pembelajaran modern. Temuan tersebut menunjukkan bahwa pemanfaatan AI telah bergerak dari sekadar otomatisasi menuju dukungan pedagogis yang lebih kontekstual.

Perbandingan dengan penelitian terdahulu memperlihatkan bahwa *intelligent tutoring systems* memberikan peningkatan signifikan terhadap kualitas umpan balik, sebagaimana dijelaskan dalam [5] yang menekankan efektivitas *real-time feedback*. Kecenderungan serupa terlihat pada studi-studi yang menguraikan manfaat AI dalam memprediksi kesulitan belajar siswa melalui model *machine learning*, konsisten dengan yang ditunjukkan dalam [8]. Namun, beberapa artikel dalam analisis ini menunjukkan variasi performa sistem AI pada konteks tertentu, sebuah temuan yang tidak selalu selaras dengan klaim stabilitas yang dilaporkan dalam [11]. Ketidaksamaan ini menunjukkan bahwa efektivitas AI sangat bergantung pada kesiapan data, desain algoritma, dan konteks implementasi.

Sejumlah temuan tak terduga muncul dari kajian terhadap hambatan penerapan AI, terutama terkait isu etika dan privasi yang ditekankan dalam [9], meskipun tidak semua penelitian memasukkannya sebagai fokus utama. Variasi perhatian terhadap aspek etika menunjukkan adanya ketidakseimbangan antara pengembangan teknologi dan penyiapan regulasi, suatu pola yang berbeda dari gambaran yang digarisbawahi dalam [6]. Selain itu, munculnya temuan mengenai keterbatasan literasi digital pendidik memperlihatkan bahwa adopsi AI tidak hanya bergantung pada perangkat, tetapi juga pada kompetensi pengguna. Hal ini menegaskan bahwa efektivitas teknologi pembelajaran tidak dapat dipisahkan dari kesiapan sumber daya manusia yang mengoperasikannya.

Secara teoritis, hasil kajian ini memperluas pemahaman mengenai bagaimana integrasi AI dalam pendidikan membentuk pola baru pembelajaran yang lebih adaptif dan berbasis data. Dari sisi praktis, temuan-temuan tersebut mengindikasikan bahwa institusi pendidikan perlu mempertimbangkan aspek teknis, pedagogis, dan etis secara bersamaan agar pemanfaatan AI dapat berjalan optimal. Kajian ini juga memperlihatkan bahwa implementasi AI memiliki potensi sebagai alat evaluasi pembelajaran yang mampu mengungkap dinamika belajar siswa secara lebih mendalam. Meskipun demikian, penelitian ini memiliki keterbatasan pada jangkauan tema yang dianalisis dan keberagaman konteks publikasi, sehingga interpretasi temuan perlu dipahami dalam ruang lingkup kajian yang terbatas.

5. KESIMPULAN DAN SARAN

5.1. *Kesimpulan*

Berdasarkan systematic literature review yang telah dilakukan, dapat disimpulkan bahwa implementasi kecerdasan buatan (AI) memegang peranan vital dalam meningkatkan keamanan jaringan Internet of Things (IoT) melalui deteksi anomali. Penelitian-penelitian terkini didominasi oleh penggunaan algoritma deep learning seperti *Convolutional Neural Network* (CNN) dan *Long Short-Term Memory* (LSTM), serta model hibrida/ensemble. Pendekatan ini terbukti sangat efektif, dengan banyak studi melaporkan tingkat akurasi deteksi di atas 99% pada dataset benchmark standar. CNN unggul dalam ekstraksi fitur spasial dari lalu lintas jaringan, sementara LSTM efektif dalam menganalisis pola temporal data, menjadikan kombinasi keduanya sebagai salah satu arsitektur hibrida yang paling kuat.

Lebih lanjut, penelitian ini mengidentifikasi bahwa efektivitas sistem deteksi tidak hanya diukur dari akurasi, tetapi juga dari efisiensinya. Keterbatasan sumber daya pada perangkat IoT mendorong para peneliti untuk mengembangkan solusi keamanan yang ringan (*lightweight*) dan hemat energi. Temuan menunjukkan bahwa berbagai strategi seperti optimalisasi model, kompresi (kuantisasi), seleksi fitur, dan perbaikan arsitektur sistem berhasil mengurangi konsumsi energi dan beban komputasi secara signifikan tanpa mengorbankan performa deteksi. Dengan demikian, tren riset saat ini jelas bergerak menuju keseimbangan optimal antara akurasi deteksi yang tinggi dan efisiensi sumber daya untuk memastikan penerapan yang praktis dan berkelanjutan di lingkungan IoT.

5.2. *Saran*

Meskipun kemajuan signifikan telah dicapai, beberapa area masih memerlukan eksplorasi lebih lanjut untuk menyempurnakan sistem deteksi anomali berbasis AI di lingkungan IoT. Perkembangan ekosistem IoT yang semakin kompleks menuntut analisis yang lebih mendalam terhadap berbagai skenario

p-ISSN : 2803-1507 e-ISSN : 2803-1531

operasional yang berbeda. Variasi karakteristik perangkat dan pola komunikasi juga mengharuskan adanya peninjauan ulang terhadap kebutuhan keamanan pada setiap lingkungan implementasi. Berdasarkan analisis yang telah dilakukan, berikut adalah beberapa saran untuk penelitian di masa mendatang:

1. Pengujian pada Skenario Dunia Nyata: Sebagian besar penelitian yang dikaji masih mengandalkan dataset benchmark yang bersifat statis. Penelitian selanjutnya disarankan untuk melakukan validasi model pada lingkungan jaringan IoT yang dinamis dan heterogen di dunia nyata (real-world testbeds). Hal ini penting untuk menguji ketahanan dan adaptabilitas model terhadap serangan zero-day dan lalu lintas jaringan yang terus berubah. Validasi pada kondisi operasional nyata juga dapat mengungkap faktor lingkungan yang tidak terekam dalam dataset statis.
2. Eksplorasi *Explainable A*I (XAI): Model *deep learning* sering dianggap sebagai "kotak hitam" (*black box*), sehingga sulit untuk memahami proses pengambilan keputusannya. Mengintegrasikan teknik XAI ke dalam sistem deteksi intrusi dapat meningkatkan transparansi dan kepercayaan. Hal ini akan membantu administrator keamanan untuk memahami mengapa sebuah aktivitas dianggap anomali, sehingga mempermudah proses investigasi dan respons insiden. Penerapan XAI dalam bidang ini juga memberi peluang untuk mengembangkan metode penjelasan yang lebih sesuai dengan karakteristik lalu lintas IoT.
3. Standarisasi Metrik Efisiensi: Meskipun banyak penelitian telah mempertimbangkan efisiensi energi, metrik yang digunakan seringkali beragam (misalnya, penggunaan CPU, konsumsi daya, pemakaian memori). Perlu adanya standarisasi dalam pengukuran dan pelaporan metrik efisiensi sumber daya. Ini akan mempermudah perbandingan yang objektif antar berbagai solusi lightweight AI yang diusulkan. Konsistensi metrik ini juga memungkinkan evaluasi performa yang lebih akurat pada berbagai kondisi implementasi.
4. Pengembangan Model Adaptif dan *Online Learning*: Lingkungan IoT sangat dinamis dengan munculnya perangkat dan pola serangan baru. Penelitian mendatang dapat berfokus pada pengembangan model AI yang mampu belajar secara terus-menerus (online learning) dan beradaptasi secara mandiri terhadap perubahan kondisi jaringan, sehingga sistem keamanan tidak cepat usang dan tetap efektif seiring waktu. Model yang adaptif juga memungkinkan peningkatan ketepatan deteksi ketika pola ancaman baru muncul dalam lalu lintas jaringan.

DAFTAR PUSTAKA

[1] S. A. Nugroho and F. R. Pratama, “Pengembangan Sistem Pendeteksi Kebocoran Gas LPG Berbasis Internet of Things di Putra Laundry Ungaran,” *J. Ilm. Sist. Inf.*, vol. 4, no. 1, pp. 49–57, Jan. 2025, doi: 10.51903/2yzfj675.

[2] A. Nanjar, T. Safitri Maharani, P. A. Prastyo, M. Taufik, N. Hidayat, and I. Kharits, “Internet of Things (IoT) Integration in Telecommunication Networks: Challenges and Opportunities,” *J. Technol. Informatics Eng.*, vol. 3, no. 1, pp. 11–24, Mar. 2024, doi: 10.51903/jtie.v3i1.156.

[3] B. W. Susilo and E. Susanto, “Employing Artificial Intelligence in Management Information Systems to Improve Business Efficiency,” *J. Manag. Informatics*, vol. 3, no. 2, pp. 212–229, Aug. 2024, doi: 10.51903/jmi.v3i2.30.

[4] N. J. Singh, N. Hoque, K. R. Singh, and D. K. Bhattacharyya, “Botnet-Based IoT Network Traffic Analysis Using Deep Learning,” *Secur. Priv.*, vol. 7, no. 2, p. 355, Mar. 2024, doi: 10.1002/spy2.355.

[5] A. Nazir *et al.*, “Advancing IoT Security: A Systematic Review of Machine Learning Approaches for the Detection of IoT Botnets,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 10, p. 101820, Dec. 2023, doi: 10.1016/j.jksuci.2023.101820.

[6] M. Gelgi, Y. Guan, S. Arunachala, M. Samba Siva Rao, and N. Dragoni, “Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques,” *Sensors*, vol. 24, no. 11, p. 3571, Jun. 2024, doi: 10.3390/s24113571.

[7] E. Dritsas and M. Trigka, “A Survey on Cybersecurity in IoT,” *Futur. Internet*, vol. 17, no. 1, p. 30, Jan. 2025, doi: 10.3390/fi17010030.

[8] D. C. Muñoz and A. del C. Valiente, “A Novel Botnet Attack Detection for IoT Networks Based on

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Communication Graphs," *Cybersecurity*, vol. 6, no. 1, pp. 33-, Dec. 2023, doi: 10.1186/s42400-023-00169-6.

[9] J. Arshad, M. A. Azad, R. Amad, K. Salah, M. Alazab, and R. Iqbal, "A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT," *Electronics*, vol. 9, no. 4, p. 629, Apr. 2020, doi: 10.3390/electronics9040629.

[10] A. Alfahaid, E. Alalwany, A. M. Almars, F. Alharbi, E. Atlam, and I. Mahgoub, "Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey," *Sensors*, vol. 25, no. 11, p. 3341, May 2025, doi: 10.3390/s25113341.

[11] A. Villafranca, K. M. Thant, I. Tasic, and M.-D. Cano, "AI-Enabled IoT Intrusion Detection: Unified Conceptual Framework and Research Roadmap," *Mach. Learn. Knowl. Extr.*, vol. 7, no. 4, p. 115, Oct. 2025, doi: 10.3390/make7040115.

[12] M. Schmitt, "Securing the Digital World: Protecting Smart Infrastructures and Digital Industries With Artificial Intelligence (AI)-Enabled Malware and Intrusion Detection," *J. Ind. Inf. Integr.*, vol. 36, p. 100520, Dec. 2023, doi: 10.1016/j.jii.2023.100520.

[13] M. Fatima, O. Rehman, I. M. H. Rahman, A. Ajmal, and S. J. Park, "Towards Ensemble Feature Selection for Lightweight Intrusion Detection in Resource-Constrained IoT Devices," *Futur. Internet*, vol. 16, no. 10, p. 368, Oct. 2024, doi: 10.3390/fi16100368.

[14] D. Pati and L. N. Lorusso, "How to Write a Systematic Review of the Literature," *Heal. Environ. Res. Des. J.*, vol. 11, no. 1, pp. 15–30, Jan. 2018, doi: 10.1177/1937586717747384.

[15] J. Jose and D. V. Jose, "AS-CL IDS: Anomaly and Signature-based CNN-LSTM Intrusion Detection System for Internet of Things," *Int. J. Adv. Technol. Eng. Explor.*, vol. 10, no. 109, pp. 1622–1639, 2023, doi: 10.19101/ijatee.2022.10100187.

[16] W. Khan *et al.*, "Enhancing Security in 6G-Enabled Wireless Sensor Networks for Smart Cities: a Multi-Deep Learning Intrusion Detection Approach," *Front. Sustain. Cities*, vol. 7, p. 1580006, May 2025, doi: 10.3389/frsc.2025.1580006.

[17] M. Tawfik, "Optimized Intrusion Detection in IoT and Fog Computing Using Ensemble Learning and Advanced Feature Selection," *PLoS One*, vol. 19, no. 8, p. e0304082, Aug. 2024, doi: 10.1371/journal.pone.0304082.

[18] S. Sakraoui, A. Ahmim, M. Derdour, M. Ahmim, S. Namane, and I. Ben Dhaou, "FBMP-IDS: FL-Based Blockchain-Powered Lightweight MPC-Secured IDS for 6G Networks," *IEEE Access*, vol. 12, pp. 105887–105905, 2024, doi: 10.1109/access.2024.3435920.

[19] S. Syed Sabir Mohamed, S. Gunasekaran, R. Chinnamuthu, and G. Singh, "Dynamic Hierarchical Intrusion Detection System for Internet of Vehicle on Edge Computing Platform," *IET Commun.*, vol. 18, no. 20, p. 1778, Dec. 2024, doi: 10.1049/cmu2.12865.

[20] O. P. Olawale and S. Ebadinezhad, "Cybersecurity Anomaly Detection: AI and Ethereum Blockchain for a Secure and Tamperproof IoHT Data Management," *IEEE Access*, vol. 12, pp. 131605–131620, 2024, doi: 10.1109/access.2024.3460428.

[21] T. Alladi, V. Kohli, V. Chamola, and F. R. Yu, "A Deep Learning Based Misbehavior Classification Scheme for Intrusion Detection in Cooperative Intelligent Transportation Systems," *Digit. Commun. Networks*, vol. 9, no. 5, pp. 1113–1122, Oct. 2023, doi: 10.1016/j.dcan.2022.06.018.

[22] H. Hatamleh, A. M. A. Alnaser, S. S. Saloum, A. Sharadqeh, and J. S. Alkasassbeh, "PictureGuard: Enhancing Software-Defined Networking–Internet of Things Security with Novel Image-Based Authentication and Artificial Intelligence-Powered Two-Stage Intrusion Detection," *Technologies*, vol. 13, no. 2, p. 55, Feb. 2025, doi: 10.3390/technologies13020055.

[23] R. Khilar *et al.*, "Artificial Intelligence-Based Security Protocols to Resist Attacks in Internet of Things," *Wirel. Commun. Mob. Comput.*, vol. 2022, no. 1, p. 1440538, Jan. 2022, doi: 10.1155/2022/1440538.

[24] K. C. Chaganti, "A Scalable, Lightweight AI-Driven Security Framework for IoT Ecosystems:

Optimization and Game Theory Approaches," *IEEE Access*, vol. 13, pp. 72235–72247, 2025, doi: 10.1109/access.2025.3558623.

[25] M. Keshk, N. Koroniotis, N. Pham, N. Moustafa, B. Turnbull, and A. Y. Zomaya, "An Explainable Deep Learning-Enabled Intrusion Detection Framework in IoT Networks," *Inf. Sci. (Ny).*, vol. 639, p. 119000, Aug. 2023, doi: 10.1016/j.ins.2023.119000.

[26] M. Aidi Sharif and C. Author, "A Mechatronics System based on Feature Selection and AI for IoT Intrusion Detection Applications," *Int. J. Integr. Eng.*, vol. 14, no. 6, pp. 290–302, Nov. 2022, doi: 10.30880/ijie.2022.14.06.026.

[27] W. Villegas-Ch, J. Govea, R. Gutierrez, and A. Mera-Navarrete, "Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Scalable and Efficient Approach for Threat Detection," *IEEE Access*, vol. 13, pp. 16933–16958, 2025, doi: 10.1109/access.2025.3532800.

[28] L. Aversano, M. L. Bernardi, M. Cimitile, D. Montano, R. Pecori, and L. Veltri, "Explainable Anomaly Detection of Synthetic Medical IoT Traffic Using Machine Learning," *SN Comput. Sci. 2024 55*, vol. 5, no. 5, pp. 488-, Apr. 2024, doi: 10.1007/s42979-024-02830-4.

[29] C. Park, J. Lee, Y. Kim, J. G. Park, H. Kim, and D. Hong, "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2330–2345, Feb. 2023, doi: 10.1109/jiot.2022.3211346.

[30] B. S. Sharmila and R. Nagapadma, "Quantized Autoencoder (QAE) Intrusion Detection System for Anomaly Detection in Resource-Constrained IoT Devices Using RT-IoT2022 Dataset," *Cybersecurity*, vol. 6, no. 1, pp. 41-, Sep. 2023, doi: 10.1186/s42400-023-00178-5.

[31] S. Selvarajan *et al.*, "An Artificial Intelligence Lightweight Blockchain Security Model for Security and Privacy in IIoT Systems," *J. Cloud Comput.*, vol. 12, no. 1, pp. 38-, Mar. 2023, doi: 10.1186/s13677-023-00412-y.

[32] N. Prazeres, R. L. de C. Costa, L. Santos, and C. Rabadão, "Engineering the Application of Machine Learning in an IDS Based on IoT Traffic Flow," *Intell. Syst. with Appl.*, vol. 17, p. 200189, Feb. 2023, doi: 10.1016/j.iswa.2023.200189.

[33] E. Tuyishime, M. Martalò, P. A. Cotfas, V. Popescu, D. T. Cotfas, and A. Rekeraho, "Resource-Efficient Traffic Classification Using Feature Selection for Message Queuing Telemetry Transport-Internet of Things Network-Based Security Attacks," *Appl. Sci.*, vol. 15, no. 8, p. 4252, Apr. 2025, doi: 10.3390/app15084252.

[34] J. Xie, "Application Study on the Reinforcement Learning Strategies in the Network Awareness Risk Perception and Prevention," *Int. J. Comput. Intell. Syst.*, vol. 17, no. 1, pp. 112-, May 2024, doi: 10.1007/s44196-024-00492-x.

[35] X. Fang *et al.*, "Pioneering Advanced Security Solutions for Reinforcement Learning-Based Adaptive key Rotation in Zigbee Networks," *Sci. Rep.*, vol. 14, no. 1, pp. 13931-, Jun. 2024, doi: 10.1038/s41598-024-64895-8.

[36] S. Adilzhanova, M. Kunelbayev, G. Amirkhanova, Y. Zhussupov, and A. Tortay, "Development of a Data Collection and Storage System for Remote Monitoring and Detection of Security Threats in the Enterprise," *Int. J. Innov. Res. Sci. Stud.*, vol. 8, no. 2, pp. 176–196, Mar. 2025, doi: 10.53894/ijirss.v8i2.5136.

[37] J. G. Almaraz-Rivera, J. A. Perez-Diaz, J. A. Cantoral-Ceballos, J. F. Botero, and L. A. Trejo, "Toward the Protection of IoT Networks: Introducing the LATAM-DDoS-IoT Dataset," *IEEE Access*, vol. 10, pp. 106909–106920, 2022, doi: 10.1109/access.2022.3211513.

[38] D. M. Ngo *et al.*, "HH-NIDS: Heterogeneous Hardware-Based Network Intrusion Detection Framework for IoT Security," *Futur. Internet*, vol. 15, no. 1, p. 9, Dec. 2022, doi: 10.3390/fi15010009.