Karapan Network Journal

Vol.X, No.X, January/Mei/July/October XXXX
Available online at: https://ejournal.omahtabing.com/index.php/knj/id

Solusi Pembelajaran Mesin untuk Keamanan Jaringan Sensor Nirkabel

Mohammad Rizki Khoirur Rofi [1)*], Imam Ghozeli [2)]

[1)2)] *Universitas Madura, Pamekasan, Indonesia*

[1)]rizzrof@gmail.com, [2)]imamghozeli96@gmail.com

Abstract

Perkembangan jaringan sensor nirkabel (Wireless Sensor Network/WSN) telah mendorong peningkatan adopsi sistem pemantauan dan otomasi pada berbagai sektor, termasuk industri, pertanian, kesehatan, serta keamanan sistem dasar. Namun, keterbatasan sumber daya komputasi dan energi pada node WSN menjadikan jaringan ini sangat sensitif terhadap berbagai ancaman keamanan, termasuk serangan penolakan layanan (DoS), spoofing, sinkhole, maupun manipulasi data. Dalam beberapa tahun terakhir, metode pembelajaran yang memanfaatkan machine learning mulai digunakan sebagai mekanisme peningkatan kemampuan deteksi, respons, dan mitigasi serangan pada WSN. Penelitian ini menyajikan tinjauan komprehensif mengenai metode pembelajaran mesin yang digunakan dalam pengamanan WSN, mencakup supervised learning, unsupervised learning, deep learning, serta pendekatan berbasis model transformer modern. Selain itu, penelitian ini meninjau tantangan implementasi ML pada lingkungan WSN yang terbatas daya, serta peluang integrasi ML dengan edge computing dan teknologi IoT generasi terbaru. Hasil tinjauan menunjukkan bahwa metode ML mampu meningkatkan tingkat deteksi serangan hingga lebih dari 95% pada beberapa arsitektur WSN. Studi ini diharapkan menjadi rujukan yang memperkuat arah pengembangan WSN yang adaptif, aman, dan andal pada berbagai skenario aplikasi berbasis IoT di masa mendatang.

Keywords: Wireless Sensor Network, Keamanan Jaringan, Machine Learning, IoT, Intrusion Detection.

Article history: Received 5 April 20XX, first decision 22 April 20XX, accepted 22 August 20XX, available online 28 October 20XX

I. PENDAHULUAN

Perkembangan teknologi komputasi dan komunikasi nirkabel telah menghasilkan pertumbuhan signifikan pada penerapan sistem Internet of Things (IoT) di berbagai domain. Salah satu komponen penting dalam ekosistem IoT adalah Wireless Sensor Network (WSN), yaitu jaringan sensor terdistribusi yang mampu mengumpulkan, memproses, dan mengirimkan data lingkungan secara mandiri[1], [2]. Penerapan WSN telah meluas pada pertanian presisi, industri manufaktur, rumah pintar, transportasi cerdas, hingga sistem keamanan kritis. Namun, peningkatan konektivitas dan integrasi berbagai perangkat IoT juga meningkatkan risiko keamanan data dan kerentanan jaringan[3], [4], [5]. WSN umumnya terdiri dari node sensor berdaya rendah yang mengandung keterbatasan dalam kemampuan komputasi, penyimpanan, dan energi. Keterbatasan ini menyebabkan WSN sensitif terhadap berbagai bentuk serangan, seperti serangan Denial-of-Service (DoS), Distributed DoS (DDoS), spoofing, sinkhole, selective forwarding, serta manipulasi paket. Pada lingkungan industri, ancaman tersebut dapat mengganggu operasi, menurunkan efisiensi produksi, dan meningkatkan risiko keselamatan kerja. Demikian pula, pada sektor infrastruktur publik, serangan siber terhadap node sensor dapat menyebabkan dampak jangka panjang yang signifikan terhadap keamanan system[6], [7], [8]. Pendekatan keamanan tradisional seperti firewall, enkripsi sederhana, dan aturan akses statis terbukti tidak cukup dalam menghadapi karakter serangan modern yang semakin canggih. Untuk mengatasi hal tersebut, pembelajaran mesin (machine learning/ML) mulai diterapkan dalam sistem keamanan jaringan guna mendeteksi pola anomali, mengidentifikasi serangan, dan melakukan klasifikasi trafik jaringan secara otomatis[9], [10]. ML mampu beradaptasi terhadap perubahan pola trafik, mengenali perilaku mencurigakan, serta mempelajari karakteristik serangan baru yang belum diidentifikasi sebelumnya.

Berbagai penelitian menunjukkan bahwa integrasi ML dalam keamanan jaringan IoT dapat meningkatkan akurasi deteksi hingga lebih dari 99%, seperti pada metode Mesin vektor pendukung, Metode pengelompokan banyak decision tree, Jaringan saraf dalam, dan model Transformer[11], [12]. SVM terbukti efektif dalam mendeteksi serangan berbasis paket dan trafik abnormal pada jaringan sensor, sementara metode Random Forest mampu mengolah dataset besar dengan tingkat generalisasi yang baik. Selain itu, model deep learning seperti CNN dan transformer memberikan performa tinggi dalam ekstraksi fitur otomatis dan deteksi intrusi pada jaringan IoT berskala besar. Dalam konteks WSN, tantangan utama penerapan ML adalah keterbatasan energi, karena proses komputasi ML memerlukan volume data yang besar. Dengan demikian, muncul pendekatan strategis seperti edge

* Mohammad Rizki Khoirur Rofi

ISSN 2443-2xxx (online) 2598-6xxx (print)
doi: http://dx.doi.org/10.20473/KNJ.X.X.pp-pp

computing, federated learning, dan optimasi model lightweight untuk mengurangi beban komputasi di tingkat node[13]. Tren riset terbaru juga mengarah pada penggunaan mekanisme hybrid antara ML dan teknik kriptografi modern untuk memperkuat proteksi data sensor[14]. Melihat pentingnya pengamanan WSN terhadap ancaman siber dan pesatnya perkembangan metode pembelajaran mesin, penelitian ini bertujuan untuk menyajikan tinjauan komprehensif mengenai solusi ML untuk keamanan WSN. Tinjauan ini mencakup klasifikasi serangan pada WSN, algoritma ML yang umum digunakan, serta tantangan implementasi pada perangkat berdaya rendah. Sehingga, penelitian ini diharapkan dapat memberikan kontribusi terhadap perancangan sistem WSN yang lebih terjamin, responsif, dan efisien dalam menghadapi ancaman keamanan modern[15], [16], [17].

II. TINJAUAN PUSTAKA

Keamanan pada WSN dapat dianggap sebagai salah satu isu penting dalam pengembangan sistem Internet of Things (IoT) modern. WSN terdiri atas sekumpulan node sensor yang saling terhubung dan mampu melakukan sensing, pemrosesan, serta komunikasi nirkabel untuk mengirimkan data ke sink node atau server pusat. Pada berbagai aplikasinya, seperti sistem industri, kesehatan, pertanian, dan transportasi[18], [19], WSN memainkan peran sentral dalam menyediakan data real-time yang diperlukan untuk pengambilan keputusan operasional. Namun, karakteristik WSN yang terbatas dalam hal energi, memori, dan kemampuan komputasi menyebabkan jaringan ini rentan terhadap berbagai ancaman keamanan yang semakin kompleks[20], [21]. Secara umum, kerentanan WSN dapat dibagi menjadi beberapa kategori, yaitu network layer attacks, physical layer attacks, dan application-layer threats. Serangan pada lapisan jaringan seperti sinkhole, selective forwarding, sybil, dan flooding dapat menyebabkan gangguan komunikasi, hilangnya paket, manipulasi data, hingga penurunan kinerja jaringan secara keseluruhan. Pada lapisan fisik, perangkat sensor dapat disabotase, diganti, atau diretas secara langsung[22], [23]. Sementara pada lapisan aplikasi, ancaman berupa spoofing, manipulasi trafik, dan penyadapan data menjadi tantangan yang terus meningkat. Untuk menjawab tantangan tersebut, berbagai pendekatan keamanan telah dikembangkan, termasuk penggunaan firewall, metode enkripsi, serta sistem deteksi intrusi tradisional. Namun, keterbatasan sumber daya WSN membuat metode konvensional tidak cukup efisien dalam menangani serangan modern yang bersifat dinamis dan variatif[24], [25], [26]. Oleh sebab itu, metode berbasis machine learning (ML) mulai diterapkan sebagai solusi untuk mendeteksi dan menganalisis pola serangan secara adaptif[27], [28], [29].

Pendekatan ML pada keamanan WSN dapat diklasifikasikan menjadi tiga pendekatan utama, yaitu supervised learning, unsupervised learning, dan deep learning[30]. Metode supervised learning, termasuk SVM, KNN, Random Forest, dan Naïve Bayes menjadi pilihan populer untuk klasifikasi serangan jaringan. SVM, misalnya, terbukti efektif dalam mendeteksi serangan DDoS dan anomali trafik dengan akurasi yang dapat mencapai lebih dari 95%. Metode Random Forest digunakan secara luas karena kemampuannya dalam menangani dataset besar dan menghasilkan performa klasifikasi yang stabil[31], [32]. Dalam pendekatan pembelajaran mandir, clustering seperti halnya K-Means dan DBSCAN digunakan untuk mengenali pola trafik abnormal tanpa memerlukan dataset berlabel. Pendekatan ini cocok untuk WSN dengan trafik dinamis dan minim informasi mengenai tipe serangan sebelumnya. Sementara itu, metode deep learning, seperti CNN dan LSTM dan model Transformer mampu mengekstraksi fitur secara otomatis dari aliran data jaringan yang kompleks, meningkatkan akurasi deteksi, serta mempercepat proses identifikasi intrusi. Penelitian terkini menunjukkan bahwa deep learning dapat mencapai akurasi hingga lebih dari 99% dalam mendeteksi serangan pada ekosistem IoT dan WSN[33], [34].

Selain pembelajaran terpusat, konsep edge computing dan federated learning semakin relevan dalam pengembangan WSN modern. Edge computing memungkinkan pemrosesan data dilakukan di tingkat node atau cluster head sehingga mengurangi kebutuhan pengiriman data ke server pusat. Federated learning memungkinkan node melakukan proses pelatihan model tanpa perlu membagikan data mentah, sehingga meningkatkan privasi dan keamanan jaringan[35], [36], [37]. Beragam penelitian menekankan pentingnya kombinasi ML, protokol keamanan responsif, serta manajemen energi yang efisien dalam membangun WSN yang aman dan berkelanjutan. Kombinasi tersebut diyakini mampu memberikan perlindungan yang maksimal terhadap serangan modern, sekaligus menjaga konsistensi performa jaringan dalam jangka panjang[38], [39].

III. METODE

A. Desain Penelitian

Riset ini disusun dengan menggunakan kerangka systematic literature review untuk mengevaluasi berbagai solusi pembelajaran mesin yang digunakan dalam pengamanan jaringan sensor nirkabel. Proses penelitian dirancang untuk mengidentifikasi metode ML yang paling relevan, tantangan implementasi, serta tren terkini pada keamanan WSN. Tahapan penelitian pada studi ini disusun mengikuti empat langkah utama[40], [41], [42], yaitu:

1) Identifikasi Sumber Literatur

Literatur dikumpulkan diambil dari jurnal nasional, jurnal internasional, dan prosiding ilmiah, beserta laporan teknis yang sesuai dengan topik keamanan WSN dan pembelajaran mesin.

2) Seleksi Literatur

Artikel diseleksi berdasarkan kriteria inklusi: keterkaitan dengan WSN, keamanan jaringan, pembelajaran mesin, atau IoT. Artikel yang tidak menyediakan hasil eksperimen atau tidak relevan dengan keamanan jaringan dikeluarkan dari daftar.

3) Analisis Konten

Thartikel dianalisis untuk mengekstraksi informasi terkait metode ML, dataset yang digunakan, metrik evaluasi, serta efektivitas dalam mendeteksi serangan.

4) Sintesis Temuan

Hasil analisis disintesis untuk menghasilkan gambaran menyeluruh mengenai tren dan tantangan implementasi ML pada keamanan WSN.

B. Parameter Analisis

Untuk menjaga konsistensi analisis, beberapa parameter digunakan sebagai acuan pada proses penelitian ini.

Parameter	Nilai / Keterangan	Deskripsi
Jenis Serangan	DoS, DDoS, Spooting, Sinkhole, Selective Forwarding	Serangan utama yang menjadi fokus deteksi
Algoritma ML	SVM, KNN, RF, CN, LSTM, Transform	Model pembelajaran mesin yang dianalisis
Dataset	CICIDS, IoT23, CICIoMT, KDD9	Dataset umum untuk pelatihan dan pengujian ML
Metrik Evaluasi	kurasi, Presisi, Recall, F-1 Score, AUC	Parameter untuk mengukur efektivitas deteksi
Lingkungan Implementasi	Node WSN, Edge Computing, Server	Lokasi pemrosesan model ML
Konsumsi Energi	Rendah – Sedang	Dampak pemrosesan ML pada daya nod

Tabel 1. Parameter analisis keamanan WSN

C. Diagram Alir Penelitian

Flowchart berikut disesuaikan dengan gaya penjelasan pada jurnal referensi, tanpa gambar eksternal, dan menggambarkan tahapan penelitian secara sistematis.

Gambar 2. Flowchat alur penelitian

Alur penelitian dimulai dari tahap awal (Mulai) yang menandai dimulainya keseluruhan proses penelitian. Tahap selanjutnya adalah pengumpulan literatur, yaitu menghimpun berbagai sumber ilmiah seperti jurnal, prosiding, dan

publikasi relevan yang membahas keamanan Wireless Sensor Network (WSN) serta penerapan algoritma pembelajaran mesin[43], [44], [45]. Literatur yang telah dikumpulkan kemudian diseleksi berdasarkan kriteria tertentu, seperti relevansi topik, tahun publikasi, dan metode yang digunakan, untuk memastikan kualitas dan kesesuaian data yang dianalisis. Setelah proses seleksi, dilakukan analisis terhadap algoritma pembelajaran mesin dan jenis serangan yang dibahas dalam setiap artikel terpilih. Analisis ini bertujuan untuk memahami karakteristik algoritma, pola serangan, serta efektivitas metode deteksi yang diterapkan. Tahap berikutnya adalah sintesis dan evaluasi, yaitu mengintegrasikan hasil analisis dari berbagai sumber untuk membandingkan kinerja metode yang ada dan menilai kelebihan serta keterbatasannya. Berdasarkan hasil sintesis tersebut, penelitian dilanjutkan dengan penyusunan laporan yang memuat temuan, pembahasan, dan kesimpulan penelitian. Alur penelitian kemudian diakhiri pada tahap selesai sebagai penutup seluruh rangkaian kegiatan penelitian[46], [47], [48].

D. Prosedur Analisis

Prosedur analisis dalam penelitian ini dilakukan secara sistematis dan terstruktur. Tahap awal dimulai dengan pengelompokan artikel berdasarkan jenis algoritma pembelajaran mesin yang digunakan, yaitu supervised learning, unsupervised learning, dan deep learning. Selanjutnya, dilakukan evaluasi terhadap efektivitas masing-masing algoritma dengan meninjau tingkat akurasi serta berbagai metrik evaluasi lainnya yang relevan. Tahap berikutnya adalah analisis terhadap tantangan implementasi algoritma pada lingkungan Wireless Sensor Network (WSN), yang mencakup aspek konsumsi energi, kompleksitas komputasi, serta keterbatasan perangkat keras. Berdasarkan seluruh hasil analisis tersebut, disusun rekomendasi yang bertujuan untuk menentukan metode pembelajaran mesin yang paling sesuai dan efektif dalam meningkatkan keamanan WSN[49], [50].

IV. Hasil

Hasil tinjauan yang sistematis terhadap penerapan machine learning (ML) telah memberikan dampak positif yang signifikan dalam meningkatkan keamanan jaringan sensor nirkabel (WSNs). Secara umum, semua studi yang diteliti menyimpulkan bahwa ML dapat meningkatkan ketepatan deteksi serangan, mempercepat identifikasi anomali, dan memberikan tanggapan responsif terhadap pola serangan kompleks. Efektivitas ML tercermin dalam akurasi model rata-rata yang berkisar antara 92% hingga 100%, terutama saat menggunakan algoritma seperti model-model seperti SVM, Random Forest, DNN, dan arsitektur Transformer. Model-model ini telah terbukti mampu menganalisis pola lalu lintas yang kompleks dalam WSN dengan tingkat kesalahan yang rendah. Dalam kelompok pembelajaran terawasi, algoritma seperti SVM, K-Nearest Neighbor (KNN), dan Random Forest merupakan pendekatan yang paling sering digunakan dalam studi sebelumnya. SVM menunjukkan kinerja yang sangat baik dalam mendeteksi serangan DoS, DDoS, dan pola lalu lintas yang tidak normal dengan akurasi lebih dari 95%. Di sisi lain, Random Forest memberikan hasil yang lebih stabil pada kumpulan data besar dan mampu menghasilkan akurasi mendekati 100%. KNN, meskipun sederhana, tetap relevan untuk skenario WSN skala kecil, meskipun memiliki kelemahan dalam proses perhitungan saat kumpulan data menjadi lebih besar. Secara keseluruhan, pembelajaran terawasi dianggap efektif karena ketersediaan kumpulan data berlabel yang semakin meningkat dalam penelitian keamanan jaringan.

Pendekatan pembelajaran tanpa pengawasan seperti K-Means dan DBSCAN juga menunjukkan hasil yang positif, terutama dalam kondisi jaringan yang tidak memiliki banyak data berlabel. K-Means mampu mengenali pola lalu lintas yang tidak biasa dengan akurasi yang konsisten, sementara DBSCAN terbukti lebih responsif dalam mendeteksi kluster anomali dalam kondisi lalu lintas yang sangat kompleks. Meskipun tingkat akurasi pembelajaran tanpa pengawasan umumnya berkisar antara 80–90%, pendekatan ini tetap relevan karena dapat mendeteksi serangan baru tanpa memerlukan proses pelatihan yang rumit. Hasil yang lebih jelas terlihat pada pendekatan deep learning. Model seperti Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), dan arsitektur Transformer secara stabil memberikan akurasi di atas 96%. CNN menunjukkan hasil yang kuat dalam mengambil fitur dari paket data, sementara LSTM unggul dalam analisis lalu lintas berurutan. Model Transformer memberikan hasil terbaik berkat kemampuannya menangkap ketergantungan jangka panjang dan pola kompleks dalam data lalu lintas WSN, yang menghasilkan tingkat false positive yang rendah. Hal ini menegaskan bahwa deep learning adalah pendekatan masa depan dalam pengembangan sistem pengenalan intrusi berbasis ML (IDS) untuk WSN.

Dalam analisis berdasarkan kumpulan data, ditemukan bahwa model pembelajaran mesin (ML) mencapai performa tertinggi pada kumpulan data modern seperti CICIDS2018, IoT23, dan CICIoMT2024. Kumpulan data klasik seperti KDD99 masih digunakan dalam beberapa studi, tetapi kurang mewakili kondisi serangan modern. Random Forest dan DNN bahkan mampu mencapai ketepatan 100% pada dataset CICIoMT2024, menjadikannya salah satu kumpulan data paling relevan untuk penelitian terbaru dalam keamanan Jaringan Sensor Nirkabel (WSN). Temuan ini menunjukkan bahwa kualitas kumpulan data memainkan peran penting dalam efektivitas model ML. Selain efektivitas algoritma, penelitian ini juga menemukan sejumlah tantangan dalam menerapkan ML pada Jaringan Sensor Nirkabel (WSN). Batasan energi pada node WSN menjadi hambatan utama karena proses komputasi ML cenderung membutuhkan banyak daya. Batasan kemampuan komputasi dan memori pada node juga membatasi penggunaan model yang lebih rumit, sehingga memerlukan pendekatan seperti komputasi tepi dan model ringan. Selain itu,

pengiriman data secara terus-menerus ke server pusat dapat membebani jaringan dan meningkatkan potensi risiko privasi. Oleh karena itu, federated learning muncul sebagai solusi yang relevan untuk melatih model ML secara tersebar tanpa perlu mengirimkan data mentah dari setiap node sensor. Secara keseluruhan, sintesis penelitian menunjukkan bahwa penggabungan antara ML, optimasi energi, dan protokol keamanan adaptif merupakan pendekatan paling tepat dalam membangun jaringan sensor nirkabel (WSN) yang aman dan berkelanjutan. Integrasi machine learning telah terbukti secara signifikan membantu meningkatkan kemampuan deteksi serangan modern, sekaligus memberikan fleksibilitas dalam menghadapi ancaman yang terus berkembang di lingkungan WSN.

V. PEMBAHASAN

Pembahasan pada penelitian ini difokuskan pada analisis efektivitas berbagai metode pembelajaran mesin dalam meningkatkan keamanan jaringan sensor nirkabel (WSN). Berdasarkan hasil sintesis literatur, terdapat tiga aspek utama yang memengaruhi performa deteksi serangan pada WSN, yaitu pemilihan algoritma pembelajaran mesin, karakteristik serangan, dan keterbatasan sumber daya perangkat. Aspek pertama berkaitan dengan optimasi algoritma pembelajaran mesin. Metode supervised learning seperti SVM, Random Forest (RF), dan KNN terbukti memiliki tingkat akurasi tinggi untuk mendeteksi serangan berbasis trafik, terutama serangan DoS, spoofing, dan sinkhole. Beberapa penelitian menunjukkan bahwa SVM mampu mencapai akurasi hingga 99,8% untuk mendeteksi serangan sekumpulan data jaringan IoT, sedangkan Random Forest menampilkan kemampuan generalisasi yang baik terhadap dataset besar seperti CICIDS dan KDD99. Namun, metode supervised membutuhkan dataset berlabel yang memadai, sehingga kurang efisien dalam lingkungan WSN yang dinamis. Pada pendekatan unsupervised learning, metode seperti K-Means dan DBSCAN dapat mengidentifikasi anomali tanpa memerlukan pelabelan data. Hal ini memberikan keunggulan dalam kondisi jaringan yang tidak memiliki informasi lengkap mengenai tipe serangan. Namun, tingkat akurasi metode ini bervariasi tergantung pada distribusi data dan parameter clustering. Metode deep learning seperti CNN, LSTM, dan transformer menjadi pendekatan paling menjanjikan dalam deteksi intrusi modern. CNN mampu mengekstraksi fitur kompleks dari trafik jaringan, sedangkan LSTM unggul dalam menganalisis urutan waktu dari aliran data sensor. Model transformer menunjukkan performa terbaik, terutama dalam mendeteksi serangan multi-vektor dengan akurasi lebih dari 96%. Meskipun demikian, metode deep learning memerlukan komputasi tinggi sehingga kurang cocok untuk node WSN yang memiliki sumber daya terbatas.

Aspek kedua yang dianalisis adalah karakteristik serangan pada WSN. Serangan DoS dan DDoS menjadi ancaman paling umum dan paling merusak karena dapat menguras energi node secara cepat melalui flooding paket. Serangan spoofing memanfaatkan pemalsuan identitas node sehingga mengganggu rute komunikasi, sedangkan serangan sinkhole dapat menarik trafik ke node berbahaya dan menciptakan manipulasi data. Pembelajaran mesin terbukti efektif dalam mengenali pola-pola serangan ini dengan memanfaatkan fitur trafik seperti interval paket, frekuensi komunikasi, dan variasi sinyal. Aspek terakhir yang menjadi tantangan utama adalah keterbatasan energi dan komputasi pada node WSN. Proses pelatihan model ML membutuhkan sumber daya besar, sehingga solusi realistis berada pada implementasi berbasis edge computing dan cluster head-level processing. Beberapa penelitian merekomendasikan penggunaan model ringan seperti SVM linear atau Random Forest dengan jumlah pohon kecil untuk memperpanjang umur jaringan. Selain itu, penggunaan federated learning mampu mengurangi kebutuhan pengiriman data ke server pusat, sehingga memperkecil konsumsi daya dan meningkatkan privasi. Secara keseluruhan, pembelajaran mesin memberikan kontribusi signifikan dalam meningkatkan keamanan WSN, tetapi pemilihan algoritma harus mempertimbangkan keterbatasan sumber daya perangkat, jenis serangan, serta profil trafik jaringan. Integrasi antara ML, manajemen energi adaptif, dan protokol keamanan modern menjadi strategi utama dalam membangun WSN yang aman dan berkelanjutan.

VI. KESIMPULAN

Berdasarkan hasil tinjauan literatur, dapat disimpulkan bahwa machine learning (ML) memiliki peran penting dalam meningkatkan keamanan jaringan sensor nirkabel (WSN) pada berbagai aplikasi Internet of Things (IoT). Penerapan ML memungkinkan proses identifikasi serangan yang lebih tepat, cepat, dan responsif dibandingkan dengan pendekatan keamanan secara statis konvensional. Algoritma berbasis pembelajaran terawasi seperti Support Vector Machine (SVM), K-Nearest Neighbor (KNN), dan Random Forest telah terbukti terbukti efektif dalam mendeteksi pola serangan umum seperti DoS, DDoS, spoofing, dan anomali lalu lintas, dengan tingkat akurasi mencapai lebih dari 95%. Di sisi lain, pendekatan deep learning, khususnya model CNN, LSTM, dan Transformer, menunjukkan kinerja tertinggi dengan tingkat ketepatan hingga 99% dalam menganalisis data jaringan yang rumit, menjadikannya solusi yang sangat menjanjikan untuk sistem keamanan WSN berskala besar.

Namun, tantangan utama dalam menerapkan ML pada Jaringan Sensor Nirkabel (WSN) adalah keterbatasan sumber daya node sensor, seperti energi, daya komputasi, dan kapasitas memori. Kerumitan tinggi algoritma ML berpotensi membebani node dan mengurangi umur kerja jaringan. Oleh karena itu, strategi seperti komputasi tepi, model ringan,

dan pembelajaran terpusat sangat penting untuk mengatasi keterbatasan ini. Pendekatan ini tidak hanya mengurangi beban kerja komputasi pada node, tetapi juga meningkatkan privasi dan meningkatkan efisiensi komunikasi di dalam jaringan. Secara keseluruhan, hasil penelitian ini membuktikan bahwa integrasi ML ke dalam sistem keamanan Jaringan Sensor Nirkabel (WSN) merupakan langkah penting yang dapat mengatasi tantangan keamanan siber modern. Kombinasi algoritma ML adaptif, optimasi sumber daya perangkat, dan pengembangan perlindungan keamanan yang responsif menjadi landasan utama dalam menciptakan WSN yang aman, tangguh, dan berkelanjutan. Penelitian lebih lanjut disarankan untuk mengeksplorasi model ML yang lebih efisien, pengujian di lingkungan WSN nyata, serta pengembangan mekanisme keamanan gabungan guna menghadapi ancaman siber yang semakin rumit di masa depan.

Kontribusi Penulis:Mohammad Rizki Hoirur Rofi bertanggung jawab atas konseptualisasi penelitian, perancangan metodologi, penulisan naskah awal (writing – original draft), penyuntingan naskah (writing – riview & editing), serta supervise keseluruhan proses penelitian. Imam Ghozeli berkontribusi dalam pengembangan perangkat lunak (software), pelaksanaan eksperimen dan pengujian system (investigation), kurasi dan pengolahan data (data curation),

Semua penulis telah membaca dan menyetujui versi naskah yang telah diterbitkan.

-Pendanaan:-
-Ucapan terimakasih:-
-Konflik Kepentingan: Para penulis menyatakan tidak mempunyai konflik kepentingan
-Ketersediaan Data:-
-Persetujuan Berdasarkan Informasi:-
-ORCID: Tidaktersedia
Penulis Pertama:-
Penulis kedua:-

REFRENSI

[1] F. P. E. Putra, M. Aziz, G. Arifin, A. Rohman, A. Rizki, and A. M. Syam, "Analisis Qos & Qoe," *J. Syntax Admiration*, vol. 5, no. 1, pp. 140–145, 2024, doi: 10.46799/jsa.v5i1.973.

[2] F. P. E. Putra, U. Ubaidi, A. B. Tamam, and R. W. Efendi, "Implementation And Simulation Of Dynamic Arp Inspection In Cisco Packet Tracer For Network Security," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 340–347, 2024, doi: 10.47709/brilliance.v4i1.4199.

[3] F. P. E. Putra, U. Ubaidi, M. Aziz, M. Irfan, and R. Alim, "Improving Network Service Quality in parts of Sampang City: QoS Evaluation and User Perception of QoE," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 408–412, 2024, doi: 10.47709/brilliance.v4i1.4311.

[4] M. Khofikur R.A, F. P. Eka Putra, M. W. Ridho G, and V. Huda, "Analisis Kinerja dan Keamanan Protokol PPTP dan L2TP/IPSec VPN pada Jaringan MikroTik," *Infotek J. Inform. dan Teknol.*, vol. 8, no. 2, pp. 334–344, 2025, doi: 10.29408/jit.v8i2.30230.

[5] F. P. E. Putra, M. Surur, M. Mahendra, and G. Arifin, "Internet Network QOS Analysis at Yala Kopitiam pamekasan Using Wireshak," *Brill. Res. Artif. Intell.*, vol. 5, no. 1, pp. 190–200, 2025, doi: 10.47709/brilliance.v5i1.5940.

[6] K. Farina and S. Opti, "PENGARUH PEMANFAATAN SISTEM INFORMASI AKUNTANSI DAN PENGGUNAAN TEKNOLOGI INFORMASI TERHADAP KINERJA UMKM," *jesya*, 2023, doi: 10.36778/jesya.v6i1.1007.

[7] Y. Manan, "Sistem Integrasi Proteksi \& Manajemen Resiko Platform Fintech peer to peer (P2P) Lending dan Payment Gateway untuk Meningkatkan Akslerasi Pertumbuhan UMKM 3.0," *Ihtifaz J. Islam. Econ. Financ. Bank.*, 2019, doi: 10.12928/IJIEFB.V2I1.847.

[8] "PENGARUH PERSEPSI OWNER DAN PENGETAHUAN AKUNTANSI DALAM PENGGUNAAN SISTEM INFORMASI AKUNTANSI TERHADAP KINERJA USAHA MIKRO, KECIL, DAN MENENGAH DI PAMULANG," 2019. doi: 10.24853/BASKARA.1.2.67-80.

[9] F. P. Eka Putra, F. Muslim, N. Hasanah, Holipah, R. Paradina, and R. Alim, "Analisis Komparasi Protokol Websocket dan MQTT Dalam Proses Push Notification," *J. Sistim Inf. dan Teknol.*, pp. 63–72, 2024, doi: 10.60083/jsisfotek.v5i4.325.

[10] F. P. E. Putra, K. Mufidah, R. M. Ilhamsyah, S. A. Efendy, and S. N. R. Barokah, "Tinjauan Performa RouterOS Mikrotik dalam Jaringan Internet: Analisis Kinerja dan Kelayakan," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 903–910, 2024, doi: 10.47709/digitech.v3i2.3446.

[11] F. Prasetyo Eka Putra, S. R. Sutarsih, S. Sofiyulloh, P. Permana, and M. Umar Mansyur, "Optimalisasi Perancangan Aplikasi Manajemen Data Koloman, Di Desa Pulau Mandangin Sampang – Madura Berbasis Website," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 9, no. 2, pp. 285–294, 2024, doi: 10.36341/rabit.v9i2.4840.

[12] F. P. E. Putra, M. Dafid, and I. Syafi'i, "Firewall Implementation as a Computer Network Security Strategy for Data Protection," *Brill. Res. Artif. Intell.*, vol. 5, no. 1, pp. 291–297, 2025, doi: 10.47709/brilliance.v5i1.6162.

[13] F. P. E. Putra, U. Ubaidi, D. Mayangsari, and N. Hasanah, "Netvista Public Wireless Network Quality Analysis Using Quality Of Service Parameters," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 443–452, 2024, doi: 10.47709/brilliance.v4i1.4388.

[14] N. Rahayu, I. A. Supriyono, and E. Mulyawan, "Pembangunan Ekonomi Indonesia Dengan Tantangan Transformasi Digital," *ADI Bisnis Digit. Interdisiplin J.*, 2022, doi: 10.34306/abdi.v4i1.823.

[15] S. Anjarwati, R. R. Zaena, D. Fitrianingsih, and I. Sulistiana, "Pengaruh Digitalisasi Akuntansi terhadap Efisiensi dan Pengurangan Biaya pada Perusahaan Wirausaha UMKM di Kota Bandung," *J. Akt. Ris. Akunt. dan Keuang.*, 2023, doi: 10.52005/aktiva.v5i1.181.

[16] S. Safiuddin and F. P. E. Putra, "Strategi Efisiensi Wireless Sensor Network (WSN)," *INFORMATICS Educ. Prof. J. Informatics*, vol. 8, no. 1, p. 52, 2023, doi: 10.51211/itbi.v8i1.2441.

[17] H. Hanif, T. Hidayat, and R. N. Haryadi, "Pelatihan Keterampilan Manajemen Operasional bagi UMKM: Peningkatan Efisiensi dan Produktivitas," *Jabdimas J. Pengabdi. Masy.*, 2023, doi: 10.56457/jabdimas.v1i1.52.

[18] A. F. Muntazori, A. Listya, and M. I. Qeis, "Branding Produk UMKM Pempek Gersang," *J. Desain*, 2019, doi: 10.30998/jd.v6i3.4252.

[19] L. M. Hamza and D. Agustien, "Pengaruh Perkembangan Usaha Mikro, Kecil, dan Menengah Terhadap Pendapatan Nasional Pada Sektor UMKM di Indonesia," *J. Ekon. Pembang.*, 2019, doi: 10.23960/JEP.V8I2.45.

[20] S. Supriatna and M. Aminah, "Analisis Strategi Pengembangan Usaha Kopi Luwak (Studi Kasus UMKM Careuh Coffee Rancabali-Ciwidey, Bandung)," *J. Manag. \& Organ.*, vol. 5, pp. 227–243, 2016, doi: 10.29244/JMO.V5I3.12171.

[21] D. Donoriyanto, R. Indiyanto, N. R. J. A. R., and Y. A. Syamsiah, "Optimalisasi Penggunaan Media Sosial sebagai Sarana Promosi Online Store pada Pelaku UMKM di Kota X," *J. Abdimas Perad.*, 2023, doi: 10.54783/ap.v4i1.22.

[22] I. Hidayatullah, M. H. Khairi, I. Maulana, and F. P. Eka Putra, "Analisis Protokol Keamanan Jaringan dalam Era Internet of Things (IoT)," *Infotek J. Inform. dan Teknol.*, vol. 8, no. 2, pp. 356–366, 2025, doi: 10.29408/jit.v8i2.30257.

[23] Z. Setiawan, A. Hiswara, and H. N. Muthmainah, "Mengoptimalkan Jaringan Sensor Nirkabel dalam Aplikasi Monitor Lingkungan dengan Teknologi IoT di Indonesia," 2023. doi: 10.58812/jmws.v2i10.704.

[24] Z. Song, Y. Zhang, Y. Yu, and C. Tang, "Cooperative Positioning Algorithm Based on Manifold Gradient Filtering in UAV-WSN," 2024. doi: 10.1109/JSEN.2024.3369701.

[25] Z. Wang, L. Huang, S. Yang, X. Luo, D. He, and S. Chan, "Multi-strategy enhanced grey wolf algorithm for obstacle-aware WSNs coverage optimization," 2024. doi: 10.1016/j.adhoc.2023.103308.

[26] V. Tyagi and S. Singh, "MS-EAR: A mobile sink based energy aware routing technique for SDN enabled WSNs," 2024. doi: 10.1007/s12083-024-01757-0.

[27] B. Setiawan and A. Fadillah, "Pendampingan Penerapan Strategi Promosi Berbasis Digital Bagi UMKM Di Wilayah Kota Bogor," 2020. doi: 10.37641/jadkes.v1i1.320.

[28] K. Ramanan, S. P. Ramesh, C. S. Kingsly, G. V. Rajkumar, D. D. N. Ponkumar, and M. Vargheese, "Sparse Long Short-Term Memory Approach for Energy-Efficient Adaptive Cluster Fuzzy-based Controller in Wireless Sensor Network," 2023. doi: 10.1109/ICSSIT55814.2023.10061129.

[29] K. Ramkumar, L. H. Alzubaidi, V. Malathy, T. Venkatesh, and K. C. G, "Intrusion Detection System in Wireless Sensor Networks using Modified Recurrent Neural Network with Long Short-Term Memory," 2024. doi: 10.1109/ICICACS60521.2024.10498333.

[30] A. Delhi, "Innovation in Business Management Exploring the Path to Competitive Excellence," *APTISI Trans. Manag.*, 2024, doi: 10.33050/atm.v8i1.2204.

[31] P. Yadav, S. C. Sharma, O. Singh, and V. Rishiwal, "Optimized Localization Learning Algorithm for Indoor and Outdoor Localization System in WSNs," 2023. doi: 10.1007/s11277-023-10304-8.

[32] A. Ojha, A. Jindal, and P. Chanak, "An Intelligent Indoor Emergency Evacuation System Using IoT-Enabled WSNs for Smart Buildings," 2024. doi: 10.1109/JIOT.2023.3321646.

[33] K. S. Sai, R. Bhat, M. Hegde, and J. Andrew, "A Lightweight Authentication Framework for Fault-Tolerant Distributed WSN," 2023. doi: 10.1109/ACCESS.2023.3302251.

[34] D. Mulyanti and A. Nurhayati, "PENERAPAN LITERASI KEUANGAN DAN PENGGUNAAN FINANCIAL TECHNOLOGY UNTUK MENILAI KINERJA KEUANGAN UMKM DI JAWA BARAT," *Ekono Insentif*, 2022, doi: 10.36787/jei.v16i2.887.

[35] N. I. Nizar and I. Lubis, "FINTECH DAN E COMMERCE UNTUK MENDORONG PERTUMBUHAN UMKM DAN INDUSTRI KREATIF," 2020. doi: 10.20884/1.sar.2020.5.1.3140.

[36] Murnawan, S. Lestari, R. Samihardjo, R. Virgana, and T. Sapanji, "Pelatihan Brand Identity Untuk UMKM: Meningkatkan Kesadaran Merek dan Daya Saing di Era Digital," *ABDIMASKU J. Pengabdi. Masy.*, 2023, doi: 10.33633/ja.v6i2.1247.

[37] I. M. Narsa, A. Widodo, and S. Kurnianto, "MENGUNGKAP KESIAPAN UMKM DALAM IMPLEMENTASI STANDAR AKUNTANSI KEUANGAN ENTITAS TANPA AKUNTABILITAS PUBLIK (PSAK-ETAP) UNTUK MENINGKATKAN AKSES MODAL PERBANKAN," 2012. doi: 10.20473/JEBA.V22I32012.4308.

[38] H. Chen, X. Wang, B. Ge, T. Zhang, and Z. Zhu, "A Multi-Strategy Improved Sparrow Search Algorithm for Coverage Optimization in a WSN," 2023. doi: 10.3390/s23084124.

[39] R. Kumar, S. Singh, and P. K. Singh, "A secure and efficient computation based multifactor authentication scheme for Intelligent IoT-enabled WSNs," 2023. doi: 10.1016/j.compeleceng.2022.108495.

[40] L. Yulia and W. Setianingsih, "STUDI MANAJEMEN MARKETING BERBASIS ONLINE (PENELITIAN PADA UMKM PRODUKSI MEBEL DI BABAKAN MUNCANG TAMANSARI KOTA TASIKMALAYA)," *J. MANEKSI*, 2020, doi: 10.31959/JM.V9I1.397.

[41] R. P. Astuti, K. Kartono, and R. Rahmadi, "Pengembangan UMKM melalui Digitalisasi Tekonolgi dan Integrasi Akses Permodalan," *ETHOS J. Penelit. dan Pengabdi. Kpd. Masy.*, 2020, doi: 10.29313/ethos.v8i2.5764.

[42] S. Supriyadi, A. Christian, I. Suryani, and I. Rusdi, "Pelatihan Canva Dalam Pembuatan Konten Promosi Media Sosial TikTok Pada Fatayat NU," *J. Altifani Penelit. dan Pengabdi. Kpd. Masy.*, 2022, doi: 10.25008/altifani.v2i6.290.

[43] D. Fitriani and H. Hwihanus, "PENGARUH SISTEM INFORMASI AKUNTANSI DALAM PENERAPAN SIKLUS PRODUKSI DAN PENGENDALIAN INTERNAL UNTUK MENINGKATKAN EFEKTIVITAS KINERJA UMKM," *J. Kaji. dan Penal. Ilmu Manaj.*, 2023, doi: 10.59031/jkpim.v1i1.47.

[44] M. Muhamad, "Tantangan Dan Peluang Penerapan Kebijakan Mandatory Sertifikasi Halal (Studi Implementasi Uu No. 33 Th. 2014 dan Pp No. 31 Th. 2019)," *J. Ilmu Ekon. dan Bisnis Islam*, 2020, doi: 10.24239/jiebi.v2i2.29.1-26.

[45] H. Awali, "URGENSI PEMANFAATAN E-MARKETING PADA KEBERLANGSUNGAN UMKM DI KOTA PEKALONGAN DI TENGAH DAMPAK COVID-19," *Balanc. J. Ekon. dan Bisnis Islam*, 2020, doi: 10.35905/balanca.v2i1.1342.

[46] Y. Erlanitasari, A. Rahmanto, and M. Wijaya, "Digital economic literacy micro, small and medium enterprises (SMES) go online," 2020. doi: 10.21831/informasi.v49i2.27827.

[47] S. Khairani and R. Pratiwi, "Peningkatan Omset Penjualan Melalui Diversifikasi Produk dan Strategi Promosi Pada UMKM Kerajinan Souvenir Khas Palembang," *CARADDE J. Pengabdi. Kpd. Masy.*, 2018, doi: 10.31960/CARADDE.V1I1.18.

[48] S. Rahayuningsih, "Identifikasi Penerapan Dan Pemahaman Kesehatan Dan Keselamatan Kerja Dengan Metode Hazard And Operability Study (Hazop) Pada UMKM Eka Jaya," *JATI UNIK J. Ilm. Tek. dan Manaj. Ind.*, 2019, doi: 10.30737/JATIUNIK.V2I1.274.

[49] E. Pardiansyah, M. Abduh, and Najmudin, "Sosialisasi dan Pendampingan Sertifikasi Halal Gratis (Sehati) Dengan Skema Self-Declare Bagi Pelaku Usaha Mikro di Desa Domas," *J. Pengabdi. dan Pengemb. Masy. Indones.*, 2022, doi: 10.56303/jppmi.v1i2.39.

[50] L. Z. Nasution, "Penguatan Industri Halal bagi Daya Saing Wilayah: Tantangan dan Agenda Kebijakan," 2020. doi: 10.26905/JREI.V1I2.5437.

[1] F. P. E. Putra, M. Aziz, G. Arifin, A. Rohman, A. Rizki, and A. M. Syam, "Analisis Qos & Qoe," *J. Syntax Admiration*, vol. 5, no. 1, pp. 140–145, 2024, doi: 10.46799/jsa.v5i1.973.

[2] F. P. E. Putra, U. Ubaidi, A. B. Tamam, and R. W. Efendi, "Implementation And Simulation Of Dynamic Arp Inspection In Cisco Packet Tracer For Network Security," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 340–347, 2024, doi: 10.47709/brilliance.v4i1.4199.

[3] F. P. E. Putra, U. Ubaidi, M. Aziz, M. Irfan, and R. Alim, "Improving Network Service Quality in parts of Sampang City: QoS Evaluation and User Perception of QoE," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 408–

412, 2024, doi: 10.47709/brilliance.v4i1.4311.

[4] M. Khofikur R.A, F. P. Eka Putra, M. W. Ridho G, and V. Huda, "Analisis Kinerja dan Keamanan Protokol PPTP dan L2TP/IPSec VPN pada Jaringan MikroTik," *Infotek J. Inform. dan Teknol.*, vol. 8, no. 2, pp. 334–344, 2025, doi: 10.29408/jit.v8i2.30230.

[5] F. P. E. Putra, M. Surur, M. Mahendra, and G. Arifin, "Internet Network QOS Analysis at Yala Kopitiam pamekasan Using Wireshak," *Brill. Res. Artif. Intell.*, vol. 5, no. 1, pp. 190–200, 2025, doi: 10.47709/brilliance.v5i1.5940.

[6] K. Farina and S. Opti, "PENGARUH PEMANFAATAN SISTEM INFORMASI AKUNTANSI DAN PENGGUNAAN TEKNOLOGI INFORMASI TERHADAP KINERJA UMKM," *jesya*, 2023, doi: 10.36778/jesya.v6i1.1007.

[7] Y. Manan, "Sistem Integrasi Proteksi \& Manajemen Resiko Platform Fintech peer to peer (P2P) Lending dan Payment Gateway untuk Meningkatkan Akslerasi Pertumbuhan UMKM 3.0," *Ihtifaz J. Islam. Econ. Financ. Bank.*, 2019, doi: 10.12928/IJIEFB.V2I1.847.

[8] "PENGARUH PERSEPSI OWNER DAN PENGETAHUAN AKUNTANSI DALAM PENGGUNAAN SISTEM INFORMASI AKUNTANSI TERHADAP KINERJA USAHA MIKRO, KECIL, DAN MENENGAH DI PAMULANG," 2019. doi: 10.24853/BASKARA.1.2.67-80.

[9] F. P. Eka Putra, F. Muslim, N. Hasanah, Holipah, R. Paradina, and R. Alim, "Analisis Komparasi Protokol Websocket dan MQTT Dalam Proses Push Notification," *J. Sistim Inf. dan Teknol.*, pp. 63–72, 2024, doi: 10.60083/jsisfotek.v5i4.325.

[10] F. P. E. Putra, K. Mufidah, R. M. Ilhamsyah, S. A. Efendy, and S. N. R. Barokah, "Tinjauan Performa RouterOS Mikrotik dalam Jaringan Internet: Analisis Kinerja dan Kelayakan," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 903–910, 2024, doi: 10.47709/digitech.v3i2.3446.

[11] F. Prasetyo Eka Putra, S. R. Sutarsih, S. Sofiyulloh, P. Permana, and M. Umar Mansyur, "Optimalisasi Perancangan Aplikasi Manajemen Data Koloman, Di Desa Pulau Mandangin Sampang – Madura Berbasis Website," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 9, no. 2, pp. 285–294, 2024, doi: 10.36341/rabit.v9i2.4840.

[12] F. P. E. Putra, M. Dafid, and I. Syafi'i, "Firewall Implementation as a Computer Network Security Strategy for Data Protection," *Brill. Res. Artif. Intell.*, vol. 5, no. 1, pp. 291–297, 2025, doi: 10.47709/brilliance.v5i1.6162.

[13] F. P. E. Putra, U. Ubaidi, D. Mayangsari, and N. Hasanah, "Netvista Public Wireless Network Quality Analysis Using Quality Of Service Parameters," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 443–452, 2024, doi: 10.47709/brilliance.v4i1.4388.

[14] N. Rahayu, I. A. Supriyono, and E. Mulyawan, "Pembangunan Ekonomi Indonesia Dengan Tantangan Transformasi Digital," *ADI Bisnis Digit. Interdisiplin J.*, 2022, doi: 10.34306/abdi.v4i1.823.

[15] S. Anjarwati, R. R. Zaena, D. Fitrianingsih, and I. Sulistiana, "Pengaruh Digitalisasi Akuntansi terhadap Efisiensi dan Pengurangan Biaya pada Perusahaan Wirausaha UMKM di Kota Bandung," *J. Akt. Ris. Akunt. dan Keuang.*, 2023, doi: 10.52005/aktiva.v5i1.181.

[16] S. Safiuddin and F. P. E. Putra, "Strategi Efisiensi Wireless Sensor Network (WSN)," *INFORMATICS Educ. Prof. J. Informatics*, vol. 8, no. 1, p. 52, 2023, doi: 10.51211/itbi.v8i1.2441.

[17] H. Hanif, T. Hidayat, and R. N. Haryadi, "Pelatihan Keterampilan Manajemen Operasional bagi UMKM: Peningkatan Efisiensi dan Produktivitas," *Jabdimas J. Pengabdi. Masy.*, 2023, doi: 10.56457/jabdimas.v1i1.52.

[18] A. F. Muntazori, A. Listya, and M. I. Qeis, "Branding Produk UMKM Pempek Gersang," *J. Desain*, 2019, doi: 10.30998/jd.v6i3.4252.

[19] L. M. Hamza and D. Agustien, "Pengaruh Perkembangan Usaha Mikro, Kecil, dan Menengah Terhadap Pendapatan Nasional Pada Sektor UMKM di Indonesia," *J. Ekon. Pembang.*, 2019, doi: 10.23960/JEP.V8I2.45.

[20] S. Supriatna and M. Aminah, "Analisis Strategi Pengembangan Usaha Kopi Luwak (Studi Kasus UMKM Careuh Coffee Rancabali-Ciwidey, Bandung)," *J. Manag. \& Organ.*, vol. 5, pp. 227–243, 2016, doi: 10.29244/JMO.V5I3.12171.

[21] D. Donoriyanto, R. Indiyanto, N. R. J. A. R., and Y. A. Syamsiah, "Optimalisasi Penggunaan Media Sosial sebagai Sarana Promosi Online Store pada Pelaku UMKM di Kota X," *J. Abdimas Perad.*, 2023, doi: 10.54783/ap.v4i1.22.

[22] I. Hidayatullah, M. H. Khairi, I. Maulana, and F. P. Eka Putra, "Analisis Protokol Keamanan Jaringan dalam Era Internet of Things (IoT)," *Infotek J. Inform. dan Teknol.*, vol. 8, no. 2, pp. 356–366, 2025, doi: 10.29408/jit.v8i2.30257.

[23] Z. Setiawan, A. Hiswara, and H. N. Muthmainah, "Mengoptimalkan Jaringan Sensor Nirkabel dalam Aplikasi Monitor Lingkungan dengan Teknologi IoT di Indonesia," 2023. doi: 10.58812/jmws.v2i10.704.
[24] Z. Song, Y. Zhang, Y. Yu, and C. Tang, "Cooperative Positioning Algorithm Based on Manifold Gradient Filtering in UAV-WSN," 2024. doi: 10.1109/JSEN.2024.3369701.
[25] Z. Wang, L. Huang, S. Yang, X. Luo, D. He, and S. Chan, "Multi-strategy enhanced grey wolf algorithm for obstacle-aware WSNs coverage optimization," 2024. doi: 10.1016/j.adhoc.2023.103308.
[26] V. Tyagi and S. Singh, "MS-EAR: A mobile sink based energy aware routing technique for SDN enabled WSNs," 2024. doi: 10.1007/s12083-024-01757-0.
[27] B. Setiawan and A. Fadillah, "Pendampingan Penerapan Strategi Promosi Berbasis Digital Bagi UMKM Di Wilayah Kota Bogor," 2020. doi: 10.37641/jadkes.v1i1.320.
[28] K. Ramanan, S. P. Ramesh, C. S. Kingsly, G. V. Rajkumar, D. D. N. Ponkumar, and M. Vargheese, "Sparse Long Short-Term Memory Approach for Energy-Efficient Adaptive Cluster Fuzzy-based Controller in Wireless Sensor Network," 2023. doi: 10.1109/ICSSIT55814.2023.10061129.
[29] K. Ramkumar, L. H. Alzubaidi, V. Malathy, T. Venkatesh, and K. C. G, "Intrusion Detection System in Wireless Sensor Networks using Modified Recurrent Neural Network with Long Short-Term Memory," 2024. doi: 10.1109/ICICACS60521.2024.10498333.
[30] A. Delhi, "Innovation in Business Management Exploring the Path to Competitive Excellence," *APTISI Trans. Manag.*, 2024, doi: 10.33050/atm.v8i1.2204.
[31] P. Yadav, S. C. Sharma, O. Singh, and V. Rishiwal, "Optimized Localization Learning Algorithm for Indoor and Outdoor Localization System in WSNs," 2023. doi: 10.1007/s11277-023-10304-8.
[32] A. Ojha, A. Jindal, and P. Chanak, "An Intelligent Indoor Emergency Evacuation System Using IoT-Enabled WSNs for Smart Buildings," 2024. doi: 10.1109/JIOT.2023.3321646.
[33] K. S. Sai, R. Bhat, M. Hegde, and J. Andrew, "A Lightweight Authentication Framework for Fault-Tolerant Distributed WSN," 2023. doi: 10.1109/ACCESS.2023.3302251.
[34] D. Mulyanti and A. Nurhayati, "PENERAPAN LITERASI KEUANGAN DAN PENGGUNAAN FINANCIAL TECHNOLOGY UNTUK MENILAI KINERJA KEUANGAN UMKM DI JAWA BARAT," *Ekono Insentif*, 2022, doi: 10.36787/jei.v16i2.887.
[35] N. I. Nizar and I. Lubis, "FINTECH DAN E COMMERCE UNTUK MENDORONG PERTUMBUHAN UMKM DAN INDUSTRI KREATIF," 2020. doi: 10.20884/1.sar.2020.5.1.3140.
[36] Murnawan, S. Lestari, R. Samihardjo, R. Virgana, and T. Sapanji, "Pelatihan Brand Identity Untuk UMKM: Meningkatkan Kesadaran Merek dan Daya Saing di Era Digital," *ABDIMASKU J. Pengabdi. Masy.*, 2023, doi: 10.33633/ja.v6i2.1247.
[37] I. M. Narsa, A. Widodo, and S. Kurnianto, "MENGUNGKAP KESIAPAN UMKM DALAM IMPLEMENTASI STANDAR AKUNTANSI KEUANGAN ENTITAS TANPA AKUNTABILITAS PUBLIK (PSAK-ETAP) UNTUK MENINGKATKAN AKSES MODAL PERBANKAN," 2012. doi: 10.20473/JEBA.V22I32012.4308.
[38] H. Chen, X. Wang, B. Ge, T. Zhang, and Z. Zhu, "A Multi-Strategy Improved Sparrow Search Algorithm for Coverage Optimization in a WSN," 2023. doi: 10.3390/s23084124.
[39] R. Kumar, S. Singh, and P. K. Singh, "A secure and efficient computation based multifactor authentication scheme for Intelligent IoT-enabled WSNs," 2023. doi: 10.1016/j.compeleceng.2022.108495.
[40] L. Yulia and W. Setianingsih, "STUDI MANAJEMEN MARKETING BERBASIS ONLINE (PENELITIAN PADA UMKM PRODUKSI MEBEL DI BABAKAN MUNCANG TAMANSARI KOTA TASIKMALAYA)," *J. MANEKSI*, 2020, doi: 10.31959/JM.V9I1.397.
[41] R. P. Astuti, K. Kartono, and R. Rahmadi, "Pengembangan UMKM melalui Digitalisasi Tekonolgi dan Integrasi Akses Permodalan," *ETHOS J. Penelit. dan Pengabdi. Kpd. Masy.*, 2020, doi: 10.29313/ethos.v8i2.5764.
[42] S. Supriyadi, A. Christian, I. Suryani, and I. Rusdi, "Pelatihan Canva Dalam Pembuatan Konten Promosi Media Sosial TikTok Pada Fatayat NU," *J. Altifani Penelit. dan Pengabdi. Kpd. Masy.*, 2022, doi: 10.25008/altifani.v2i6.290.
[43] D. Fitriani and H. Hwihanus, "PENGARUH SISTEM INFORMASI AKUNTANSI DALAM PENERAPAN SIKLUS PRODUKSI DAN PENGENDALIAN INTERNAL UNTUK MENINGKATKAN EFEKTIVITAS KINERJA UMKM," *J. Kaji. dan Penal. Ilmu Manaj.*, 2023, doi: 10.59031/jkpim.v1i1.47.
[44] M. Muhamad, "Tantangan Dan Peluang Penerapan Kebijakan Mandatory Sertifikasi Halal (Studi Implementasi Uu No. 33 Th. 2014 dan Pp No. 31 Th. 2019)," *J. Ilmu Ekon. dan Bisnis Islam*, 2020, doi: 10.24239/jiebi.v2i2.29.1-26.
[45] H. Awali, "URGENSI PEMANFAATAN E-MARKETING PADA KEBERLANGSUNGAN UMKM DI

KOTA PEKALONGAN DI TENGAH DAMPAK COVID-19," *Balanc. J. Ekon. dan Bisnis Islam*, 2020, doi: 10.35905/balanca.v2i1.1342.

[46] Y. Erlanitasari, A. Rahmanto, and M. Wijaya, "Digital economic literacy micro, small and medium enterprises (SMES) go online," 2020. doi: 10.21831/informasi.v49i2.27827.

[47] S. Khairani and R. Pratiwi, "Peningkatan Omset Penjualan Melalui Diversifikasi Produk dan Strategi Promosi Pada UMKM Kerajinan Souvenir Khas Palembang," *CARADDE J. Pengabdi. Kpd. Masy.*, 2018, doi: 10.31960/CARADDE.V1I1.18.

[48] S. Rahayuningsih, "Identifikasi Penerapan Dan Pemahaman Kesehatan Dan Keselamatan Kerja Dengan Metode Hazard And Operability Study (Hazop) Pada UMKM Eka Jaya," *JATI UNIK J. Ilm. Tek. dan Manaj. Ind.*, 2019, doi: 10.30737/JATIUNIK.V2I1.274.

[49] E. Pardiansyah, M. Abduh, and Najmudin, "Sosialisasi dan Pendampingan Sertifikasi Halal Gratis (Sehati) Dengan Skema Self-Declare Bagi Pelaku Usaha Mikro di Desa Domas," *J. Pengabdi. dan Pengemb. Masy. Indones.*, 2022, doi: 10.56303/jppmi.v1i2.39.

[50] L. Z. Nasution, "Penguatan Industri Halal bagi Daya Saing Wilayah: Tantangan dan Agenda Kebijakan," 2020. doi: 10.26905/JREI.V1I2.5437.