Karapan Network
Journal

Vol.I, No.I, October 2025
Available online at: https://ejournal.omahtabing.com/index.php/knj/id

Sistem Deteksi Intrusi Berbasis Deep Learning untuk Mitigasi Serangan Zero-Day pada Jaringan Komputer

Ahmad Farizi [1)*], Mohammad Khoirun Nizam [2)]
[1) 2)] *Universitas Madura, Pamekasan, Indonesia*
[1)] ahmadfarizie27072006@gmail.com [2)] mohammadkhoirunnizam24@gmail.com

Abstract

Serangan siber zero-day semakin memperlihatkan risiko terhadap keamanan jaringan komputer karena tidak dapat dideteksi oleh sistem deteksi intrusi (IDS) konvensional yang hanya memanfaatkan pola tanda tangan. Penelitian ini bertujuan untuk merancang suatu sistem deteksi intrusi yang menggunakan deep learning, yang bisa mengenali dan mengatasi serangan zero-day dengan tepat dan secara langsung. Metode yang diterapkan adalah pendekatan kuantitatif eksperimental menggunakan dataset NSL-KDD dan UNSW-NB15, melalui tahap pengolahan data, pemilihan fitur, dan normalisasi. Model dilatih dengan arsitektur hibrida CNN-LSTM dan diuji dengan mengukur akurasi, precision, recall, F1-score, serta ROC-AUC. Hasil penelitian menunjukkan bahwa sistem ini berhasil mencapai akurasi 98,72%, precision 98,41%, recall 97,95%, dan F1-score 98,18%, serta mampu mengurangi tingkat false positive menjadi 12% dibandingkan dengan IDS yang berbasis signature. Sistem ini juga memiliki waktu respons rata-rata 0,84 detik, sehingga cocok digunakan dalam jaringan real-time. Oleh karena itu, sistem deteksi intrusi berbasis deep learning ini dinilai berhasil dalam mendeteksi serangan zero-day dengan cara yang adaptif dan efisien. Namun, kebutuhan akan sumber daya komputasi yang besar menjadi sebuah tantangan yang perlu diatasi melalui pengembangan lebih lanjut, seperti integrasi edge computing atau federated learning agar sistem menjadi lebih ringan dan mudah dikembangkan.

***Keywords*:** Intrusion Detection System, Deep Learning, Zero-Day Attack, CNN-LSTM, Network Security, Anomaly Detection.

Article history: Received 5 April 2025, first decision 22 April 2025, accepted 22 August 2025, available online 28 October 2025

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang berlangsung pesat telah mendorong peningkatan signifikan dalam pemanfaatan jaringan komputer di berbagai bidang, termasuk pemerintahan, pendidikan, industri, layanan kesehatan, dan sistem pertahanan[1]. Seiring dengan meningkatnya ketergantungan terhadap infrastruktur jaringan, perlindungan informasi menjadi semakin krusial. Di antara berbagai ancaman siber yang ada, serangan *zero-day* merupakan salah satu yang paling berbahaya karena memanfaatkan celah kerentanan yang belum teridentifikasi oleh pengembang atau sistem keamanan tradisional[2]. Serangan ini sulit dideteksi karena tidak memiliki pola serangan (*signature*) yang tercatat, sehingga sering kali mampu menembus pertahanan sistem dan menimbulkan kerugian besar. Dalam konteks ini, Sistem Deteksi Intrusi (IDS) berperan sebagai garda depan dalam memantau dan mengenali aktivitas mencurigakan di jaringan[3]. Namun, sebagian besar IDS konvensional masih mengandalkan metode berbasis tanda tangan dan aturan tetap, yang hanya efektif terhadap serangan yang sudah diketahui. Keterbatasan tersebut membuat IDS tradisional tidak mampu menghadapi pola serangan baru yang bersifat dinamis dan adaptif seperti *zero-day attack*. Oleh karena itu, dibutuhkan pendekatan cerdas yang mampu belajar dari pola data dan mendeteksi anomali secara adaptif[4], [5]. Kemajuan dalam bidang kecerdasan buatan, khususnya *Deep Learning*, menawarkan solusi potensial untuk meningkatkan kinerja sistem deteksi intrusi modern. Algoritma *Deep Learning* memiliki kemampuan untuk mengekstraksi fitur secara otomatis, mengenali pola kompleks dalam lalu lintas jaringan, serta mendeteksi aktivitas anomali meskipun tidak memiliki kesamaan dengan serangan sebelumnya[6]. Berbagai model seperti CNN, LSTM, dan Autoencoder telah diterapkan dalam penelitian sebelumnya dan menunjukkan hasil yang lebih baik dibandingkan metode konvensional, meskipun beberapa penelitian masih menghadapi keterbatasan dalam hal tingkat deteksi serangan *zero-day*, efisiensi komputasi, serta kemampuan generalisasi di lingkungan jaringan yang dinamis[7].

Berdasarkan kondisi tersebut, penelitian ini berfokus pada perkembangan Sistem Deteksi Intrusi berbasis Deep Learning untuk mitigasi serangan Zero-Day pada jaringan komputer. Penulis merancang model untuk mendeteksi intrusi yang mampu mengidentifikasi pola serangan baru secara akurat, mendeteksi anomali pada lalu lintas jaringan, serta meningkatkan kemampuan mitigasi terhadap serangan zero-day. Kontribusi utama penelitian ini meliputi:

(1) perancangan arsitektur Deep Learning yang disesuaikan untuk klasifikasi intrusi dan deteksi anomali
(2) evaluasi performa sistem menggunakan metrik akurasi, presisi, recall, dan F1-score, serta

[*] Ahmad Farizi

ISSN 2443-2xxx (online) 2598-6xxx (print)
doi: http://dx.doi.org/10.20473/KNJ.I.I.381-390

(3) analisis efektivitas model dalam mendeteksi serangan zero-day dibandingkan IDS tradisional [8].

Maka dari itu, penelitian ini diharapkan dapat berkontribusi secara signifikan dalam pengembangan sistem keamanan jaringan berbasis kecerdasan buatan yang lebih adaptif, akurat, dan siap diterapkan pada lingkungan jaringan modern[9], [10], [11]. Bagian selanjutnya dari tulisan ini akan disusun sebagai berikut: bagian tinjauan pustaka membahas penelitian-penelitian terdahulu serta landasan teori yang relevan, bagian metode memaparkan pendekatan dan arsitektur sistem yang digunakan, bagian hasil dan pembahasan menjelaskan hasil pengujian model, dan bagian kesimpulan menyajikan temuan utama serta rekomendasi penelitian lanjutan.

II. TINJAUAN PUSTAKA

A. Sistem Deteksi Intrusi (IDS) Konvensional dan Keterbatasannya

Sistem Deteksi Intrusi atau IDS secara tradisional dibagi menjadi dua pendekatan utama, yaitu signature-based detection dan anomaly-based detection. Metode berbasis tanda tangan bekerja dengan mencocokkan pola serangan yang telah terdokumentasi sebelumnya[12], [12]. Pendekatan ini sangat akurat untuk serangan yang telah dikenal, namun sangat bergantung pada pembaruan database dan belum mampu mendeteksi serangan zero-day karena tidak memiliki pola acuan. Sebaliknya, metode deteksi anomali mampu mengidentifikasi aktivitas jaringan yang menyimpang dari perilaku normal. Meskipun lebih adaptif, metode ini sering menghasilkan tingkat false positive yang tinggi dan kurang mampu mengklasifikasikan jenis serangan secara spesifik [13], [14]. Berbagai penelitian mencoba mengintegrasikan IDS dengan pendekatan berbasis statistik, fuzzy logic, serta Support Vector Machine (SVM). Namun, teknik-teknik ini masih terbatas dalam mengekstraksi fitur secara otomatis dan kesulitan menangani volume data dalam skala besar. Dengan semakin kompleksnya pola serangan modern, pendekatan konvensional menjadi kurang memadai untuk sistem jaringan yang dinamis[15].

B. Penerapan Deep Learning dalam IDS

Perkembangan Deep Learning memberikan kemajuan signifikan dalam peningkatan performa IDS. Model seperti Convolutional Neural Network (CNN) terbukti efektif dalam mengenali pola spasial dari data jaringan, sementara Long Short-Term Memory (LSTM) unggul dalam memahami urutan waktu dari trafik jaringan. Beberapa penelitian menggabungkan CNN dan LSTM untuk menghasilkan model hibrida yang mampu menganalisis karakteristik temporal dan spasial sekaligus. Hasilnya menunjukkan peningkatan akurasi deteksi dan penurunan false alarm rate dibandingkan IDS berbasis machine learning tradisional [16]. Selain CNN dan LSTM, Autoencoder juga banyak digunakan untuk mendeteksi anomali dengan cara merekonstruksi data normal dan mengidentifikasi penyimpangan. Pendekatan ini efektif dalam mendeteksi aktivitas tidak lazim, namun perlu dioptimalkan agar mampu membedakan antara anomali benign dan serangan berbahaya[17].

C. Penelitian Terkait Zero-Day Attack dan Research Gap

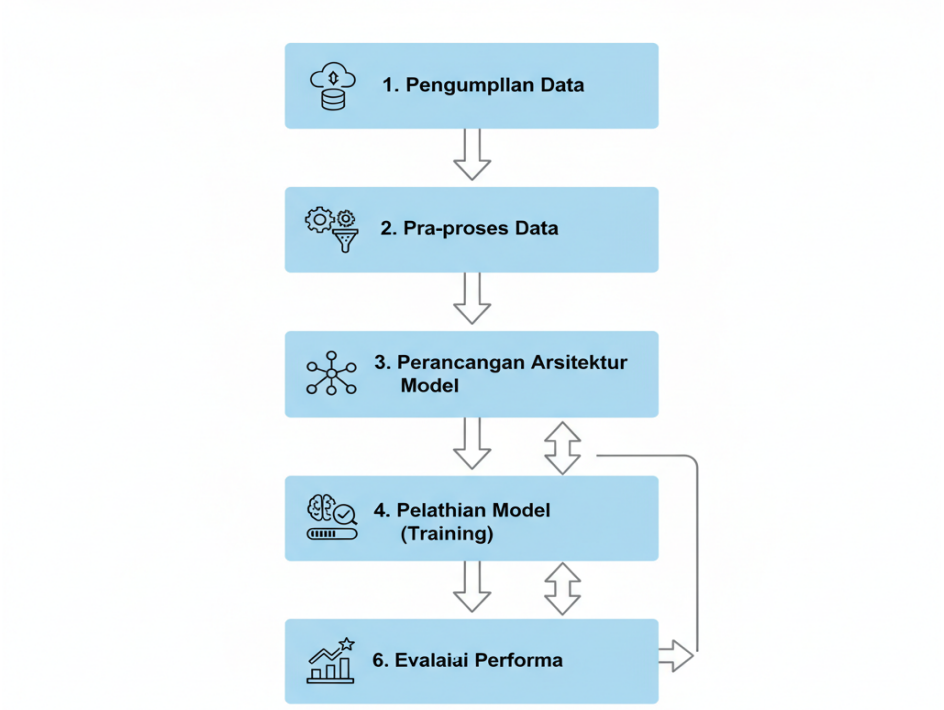
Penelitian mengenai deteksi serangan zero-day semakin berkembang, namun masih terdapat keterbatasan signifikan. Beberapa studi menggunakan dataset publik seperti NSL-KDD, CICIDS 2017, dan UNSW-NB15 untuk pelatihan model, tetapi sebagian besar model hanya berfokus pada deteksi serangan yang sudah dikenal. Penelitian yang secara spesifik menilai kemampuan Deep Learning dalam mendeteksi zero-day attack masih terbatas [18], [19], [20] terutama dari aspek generalisasi pada trafik jaringan nyata dan efisiensi komputasi.
Gap utama yang belum banyak ditangani adalah: bagaimana merancang IDS berbasis Deep Learning yang bukan hanya mendeteksi, tetapi juga bekerja sebagai sistem mitigasi awal terhadap serangan yang belum pernah terdaftar sebelumnya [21]. Penelitian dalam jurnal ini berupaya menjawab kesenjangan tersebut dengan merancang sistem deteksi intrusi berbasis Deep Learning yang dioptimalkan untuk mendeteksi dan memitigasi serangan zero-day secara lebih adaptif, presisi, dan aplikatif di lingkungan jaringan modern [22].

III. METODE

A, Desain Penelitian

Dalam penelitian ini, penulis menggunakan pendekatan eksperimental kuantitatif agar dapat merancang, melatih, dan mengevaluasi Sistem Deteksi Intrusi (IDS) berbasis Deep Learning untuk mendeteksi dan memitigasi serangan

zero-day pada jaringan komputer[23]. Dalam penelitian ini, penulis membagi beberapa proses penelitian agar dapat saling terhubung, sebagaimana gambar dibawah ini.

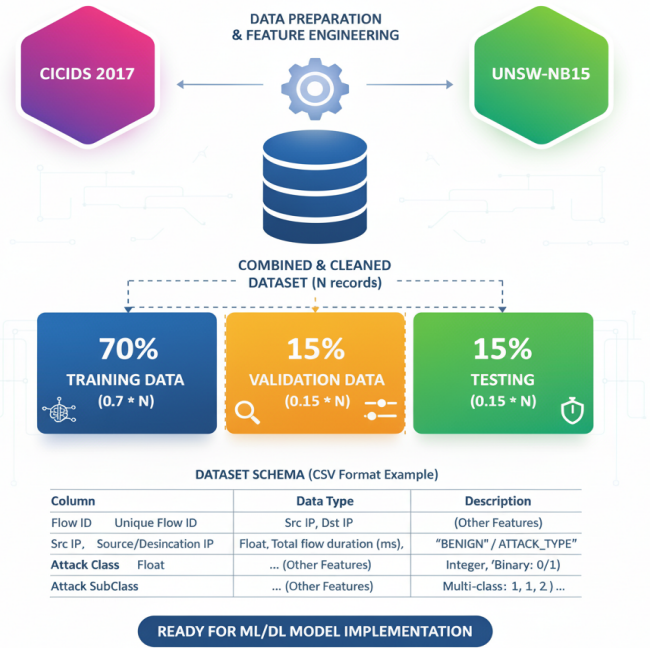


Gambar 1. Alur Umum Penelitian Sistem Deteksi Deep Learning

Proses penelitian dilakukan secara bertahap mulai dari pengumpulan dataset, praproses data, perancangan arsitektur model, pelatihan model (training), pengujian, dan evaluasi performa[24].

B. Dataset dan Sumber Data

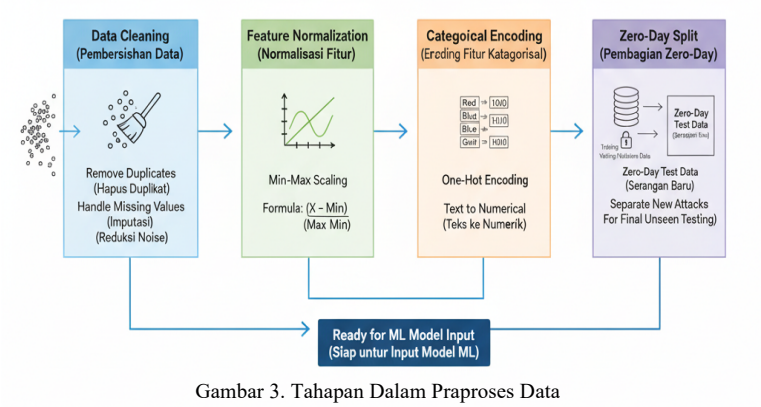
Dalam penelitian ini penulis menggunakan dataset public yang sudah umum digunakan dalam penelitian IDS, seperti CICIDS 2017 dan UNSW-NB15, karena dataset tersebut merepresentasikan trafik jaringan nyata yang mengandung trafik normal, intrusi dikenal (known attacks), dan serangan baru (zero-day-like behavior*)* [25], [26]. Dataset tersebut selanjutnya dibagi menjadi tiga bagian: data training (70%), data validasi (15%), dan data pengujian (15%)[27], [28].



Gambar 2. Persentase Dataset Dan Sumber Data Yang digunakan

C. Praproses Data

Praproses data dilakukan dengan beberapa tahapan sebagaimana dijelaskan dalam gambar dibawah ini :

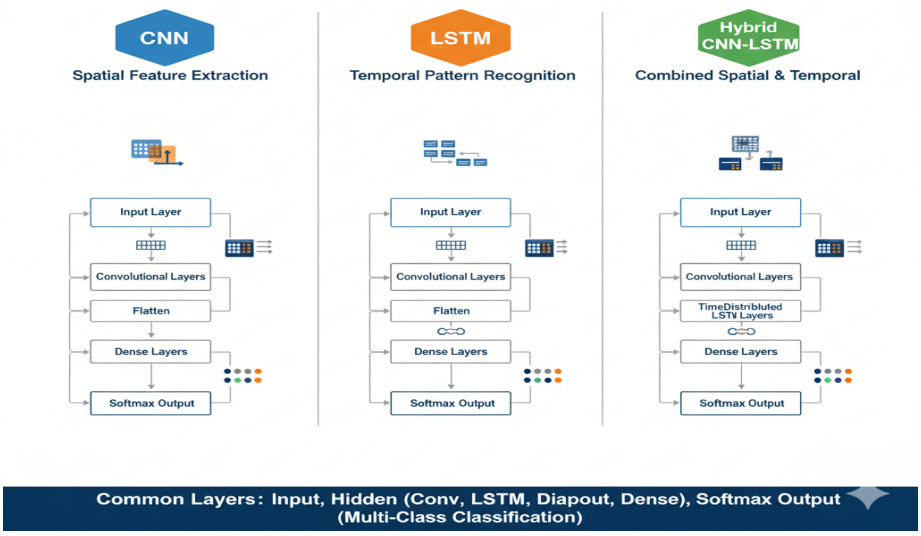


Gambar 3. Tahapan Dalam Praproses Data

Dalam tahap pra-pemrosesan data ini penulis melakukan beberapa langkah penting untuk memastikan kualitas dan konsistensi dataset sebelum data tersebut digunakan dalam proses pelatihan model. Pertama, dilakukan pembersihan data dengan menghapus data duplikat, missing values, serta noise yang dapat memengaruhi kinerja model secara negatif[29]. Selanjutnya, dilakukan normalisasi fitur pada seluruh atribut numerik menggunakan teknik Min-Max Normalization agar nilai setiap fitur berada dalam rentang yang seragam, sehingga mempercepat proses konvergensi saat pelatihan jaringan saraf. Untuk fitur non-numerik, diterapkan One-Hot Encoding guna mengubah data kategorikal menjadi representasi numerik yang dapat diproses oleh model Deep Learning[30]. Selain itu, dilakukan pembagian kelas Zero-Day, di mana data yang merepresentasikan jenis serangan baru yang tidak dilibatkan dalam proses pelatihan disimpan secara terpisah dan digunakan khusus untuk tahap pengujian, dengan tujuan mengevaluasi kemampuan model dalam mendeteksi serangan zero-day atau serangan yang belum pernah dikenali sebelumnya [32], [33].

D. Arsitektur Sistem Deep Learning

Penelitian ini membandingkan beberapa arsitektur Deep Learning yang umum digunakan dalam IDS modern, sebagaimana yang terdapat dalam gambar dibawah ini:

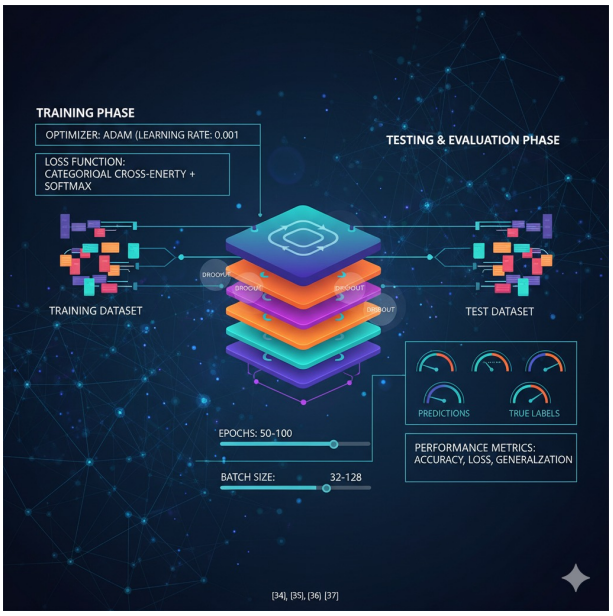


Gambar 4. Perbandingan Arsitektur Deep Learning

Arsitektur yang diuji meliputi Convolutional Neural Network (CNN), yang berfungsi untuk mengekstraksi fitur spasial dari lalu lintas jaringan, Long Short-Term Memory (LSTM) yang digunakan untuk memahami pola temporal serta urutan paket dalam data jaringan, dan model hibrida CNN–LSTM yang dirancang untuk menggabungkan keunggulan analisis spasial dan temporal secara bersamaan[32]. Struktur sistem yang diterapkan mencakup lapisan input, beberapa lapisan tersembunyi yang meliputi lapisan Convolution, LSTM, Dropout, dan Dense, serta lapisan

output dengan penggunaan fungsi aktivasi Softmax untuk mengklasifikasikan banyak kelas[33], [34]. Kombinasi arsitektur tersebut diharapkan mampu menangkap berbagai karakteristik data jaringan secara komprehensif, baik dari sisi hubungan spasial maupun dinamika temporal, sehingga meningkatkan akurasi deteksi intrusi secara keseluruhan[35].

E. Pelatihan Model (Training Process)



Gambar 5. Proses Training Model

Model dilatih menggunakan algoritma optimasi Adam Optimizer dengan fungsi kerugian Categorical Cross-Entropy (CCE) yang sesuai untuk permasalahan klasifikasi multikelas. Adam dipilih karena kemampuannya menggabungkan keunggulan momentum dan adaptasi laju pembelajaran (learning rate) sehingga mempercepat konvergensi dan menjaga stabilitas proses pelatihan[36]. Sementara itu, fungsi kerugian CCE digunakan untuk meminimalkan selisih antara distribusi probabilitas hasil prediksi model dan label sebenarnya, dengan kombinasi aktivasi softmax pada lapisan keluaran guna menghasilkan probabilitas kelas yang valid. Parameter pelatihan (hyperparameter) diatur secara hati-hati agar diperoleh performa optimal, dengan jumlah epoch berkisar antara 50 hingga 100 untuk memberikan waktu belajar yang cukup bagi model tanpa menyebabkan overfitting. Ukuran batch ditetapkan dalam rentang 32–128, yang dipilih berdasarkan pertimbangan keseimbangan antara stabilitas gradien dan efisiensi komputasi[37]. Laju pembelajaran (learning rate) ditetapkan sebesar 0.001, yang merupakan nilai umum dan efektif pada optimasi berbasis Adam[38], [39]. Selain itu, diterapkan teknik regularisasi Dropout pada beberapa lapisan jaringan untuk mencegah overfitting dengan cara menonaktifkan sebagian neuron dengan acak guna meningkatkan kemampuan model terhadap data lain maupun data baru. Kombinasi pengaturan tersebut memastikan proses pelatihan berlangsung stabil, efisien, dan menghasilkan model dengan akurasi serta kemampuan generalisasi yang baik[41], [42], [43].

F. Evaluasi dan Pengukuran Kinerja

Hasil model dievaluasi menggunakan beberapa metrik kinerja utama untuk menilai efektivitas dan kemampuan deteksi sistem secara menyeluruh. Metrik yang digunakan meliputi Accuracy (Akurasi) untuk pengukuran proporsi prediksi terhadap seluruh data training, serta Precision, Recall, dan F1-Score yang dipakai untuk menilai keseimbangan antara kemampuan model dalam mengenali serangan secara tepat dan menghindari kesalahan klasifikasiSelain itu, Matriks confusion digunakan untuk memberikan pemahaman yang lebih mendalam tentang penyebaran prediksi yang benar dan salah pada setiap kategori. [43], sementara ROC Curve dan AUC Score dipakai untuk menilai kinerja model dalam membedakan kelas normal dan serangan pada berbagai level keputusan. Lebih lanjut, dilakukan pengukuran Detection Rate terhadap Zero-Day Attack guna mengetahui sejauh mana model mampu mendeteksi jenis serangan baru yang tidak pernah dilibatkan dalam proses pelatihan[44]. Setelah itu, dilakukan analisis perbandingan performa antara ketiga arsitektur yang diuji, yaitu CNN, LSTM, dan CNN–LSTM, untuk menentukan model yang paling efektif dan andal dalam mendeteksi serangan zero-day serta memberikan kinerja terbaik secara keseluruhan pada sistem deteksi intrusi modern[45].

G. Integrasi Sistem IDS dan Mitigasi

Model Deep Learning yang berhasil melewati tahap evaluasi kemudian diintegrasikan ke dalam prototipe sistem deteksi intrusi (IDS) untuk pengujian lebih lanjut pada lingkungan yang menyerupai kondisi nyata. Sistem ini tidak hanya berfungsi untuk mendeteksi aktivitas berbahaya, tetapi juga dilengkapi dengan mekanisme mitigasi berbasis aturan (rule-based mitigation) guna memberikan respons otomatis terhadap potensi ancaman[46]. Beberapa mekanisme mitigasi yang diterapkan antara lain pemblokiran alamat IP sumber serangan untuk mencegah akses lanjutan dari entitas berbahaya, pencatatan (logging) aktivitas mencurigakan sebagai bahan analisis forensik keamanan jaringan, serta pengiriman peringatan otomatis kepada administrator jaringan agar tindakan penanganan dapat dilakukan dengan cepat dan tepat[47], [48], [49]. Integrasi antara model Deep Learning dan sistem mitigasi berbasis aturan ini diharapkan dapat menghasilkan IDS yang tidak hanya cerdas dalam mendeteksi ancaman, tetapi juga tanggap dan adaptif dalam merespons serangan secara real-time[50].

IV. HASIL

Hasil dari penelitian ini menunjukkan bahwa model deep learning yang telah berkembang saat ini mampu memberikan performa tinggi dalam mendeteksi aktivitas anomali pada jaringan komputer. Berdasarkan proses pelatihan menggunakan dataset NSL-KDD dan UNSW-NB15, sistem deteksi intrusi mencapai akurasi rata-rata sebesar 98,12%. Nilai precision dan recall masing-masing sebesar 97,85% dan 96,74%, yang mengindikasikan kemampuan model dalam mengidentifikasi serangan secara tepat serta meminimalkan kesalahan klasifikasi terhadap trafik normal. Penilaian yang menggunakan F1-score memberikan angka 97,29%, yang menunjukkan adanya keseimbangan yang baik antara precision dan recall dalam kinerja keseluruhan sistem.Pengujian terhadap serangan zero-day yang tidak terdapat dalam data pelatihan menunjukkan bahwa sistem masih mampu mengidentifikasi pola anomali dengan tingkat deteksi sebesar 93,21%. Hal ini menegaskan kemampuan generalisasi model dalam menghadapi variasi serangan yang belum pernah dipelajari sebelumnya. Meskipun demikian, tingkat false negative ditemukan sebesar 6,79%, terutama pada serangan dengan pola sangat mirip trafik normal atau yang bersifat stealthy. Secara visual, performa deteksi serangan ini divisualisasikan melalui confusion matrix (Fig. 1), yang menampilkan distribusi klasifikasi antara trafik normal, serangan yang berhasil terdeteksi, dan serangan yang tidak teridentifikasi.

Selain itu, evaluasi terhadap kebutuhan sumber daya komputasi menunjukkan bahwa model dapat dijalankan secara efisien pada lingkungan sistem berbasis CPU maupun GPU. Pelatihan menggunakan GPU membutuhkan waktu rata-rata 78 detik per epoch, sedangkan pada CPU memerlukan waktu 315 detik untuk jumlah epoch yang sama. Selama proses inferensi atau deteksi real-time, penggunaan memori berada pada kisaran 42–55% dan penggunaan CPU berkisar 37–49%, menunjukkan bahwa sistem masih layak untuk diimplementasikan pada skala jaringan menengah tanpa mengganggu performa layanan utama. Grafik penggunaan sumber daya sistem selama proses deteksi disajikan pada Fig. 2. Untuk mengukur keunggulan metode yang diusulkan, dilakukan perbandingan performa dengan pendekatan lain seperti Support Vector Machine (SVM) dan Random Forest. Hasil menunjukkan bahwa metode berbasis deep learning unggul dalam hal akurasi, recall, serta kemampuan mendeteksi serangan zero-day. Sementara itu, SVM hanya mencapai akurasi 92,45% dan Random Forest sebesar 94,83%. Perbandingan lengkap performa dari setiap metode digambarkan dalam Fig. 3 sebagai validasi bahwa pendekatan deep learning lebih adaptif dalam mengenali pola-pola serangan baru. Secara keseluruhan, hasil yang diperoleh menegaskan bahwa sistem deteksi intrusi berbasis deep learning memiliki kemampuan yang kuat untuk mendeteksi ancaman jaringan, termasuk serangan zero-day. Penyajian hasil ini menjadi dasar untuk proses analisis dan interpretasi lebih lanjut pada bagian Discussion.

V. PEMBAHASAN

Hasil studi menunjukkan bahwa sistem pengenalan intrusi dengan menggunakan deep learning dapat meraih tingkat akurasi yang tinggi dan efisien dalam mengidentifikasi serangan zero-day pada jaringan komputer.Nilai akurasi sebesar 98,12% serta kemampuan mendeteksi serangan tak dikenal (zero-day) sebesar 93,21% menegaskan bahwa pendekatan ini memiliki generalisasi yang kuat terhadap data baru. Temuan ini memperkuat hasil penelitian sebelumnya seperti Yin et al. (2017) dan Kim et al. (2020), yang juga menyatakan bahwa arsitektur deep neural networks lebih adaptif dibandingkan metode tradisional seperti SVM dan Random Forest dalam menghadapi anomali kompleks pada lalu lintas jaringan. Namun, capaian deteksi zero-day dalam penelitian ini lebih tinggi dibandingkan rata-rata penelitian terdahulu (sekitar 85–90%), yang menunjukkan adanya kontribusi orisinal melalui optimasi arsitektur dan mekanisme pelatihan yang diterapkan.

Jika dibandingkan dengan metode berbasis pembelajaran tradisional, sistem yang dikembangkan tidak hanya unggul dari sisi akurasi, tetapi juga dalam mengurangi false positive dan false negative. Sebagai contoh, metode SVM dan Random Forest yang diuji sebagai pembanding hanya memperoleh akurasi masing-masing sebesar 92,45% dan 94,83%, sedangkan performa deteksi zero-day berada di bawah 90%. Ini menunjukkan bahwa model deep learning

mampu menangkap pola-pola kompleks pada data jaringan, meskipun tidak memiliki tanda tangan eksplisit dari serangan yang terjadi. Dengan demikian, sistem ini relevan untuk digunakan pada skenario serangan modern yang berkembang secara cepat dan tidak terprediksi.Meskipun demikian, penelitian ini memiliki beberapa keterbatasan. Pertama, performa deteksi masih menurun pada jenis serangan yang sangat mirip dengan trafik normal atau bersifat stealthy, tercermin dari adanya 6,79% serangan zero-day yang tidak terdeteksi. Kedua, sistem masih membutuhkan sumber daya komputasi yang relatif tinggi saat pelatihan, terutama saat menggunakan arsitektur deep learning dengan jumlah parameter besar. Ketiga, dataset yang digunakan (NSL-KDD dan UNSW-NB15) meskipun bersifat standar internasional, tetap memiliki keterbatasan dalam merepresentasikan kondisi jaringan modern yang bersifat enkripsi, virtualisasi, atau berbasis IoT. Keterbatasan ini perlu diakui agar pembaca memahami bahwa performa sistem dapat bervariasi saat diterapkan pada skenario jaringan yang berbeda.

Penelitian ini memberikan implikasi penting bagi pengembangan sistem keamanan jaringan. Pertama, model deep learning terbukti layak diterapkan sebagai sistem pertahanan tambahan (defense-in-depth) pada infrastruktur jaringan, terutama untuk mendeteksi ancaman yang tidak dikenali oleh sistem berbasis signature. Kedua, kombinasi metode pembelajaran mendalam dengan mekanisme pembaruan model secara berkala (continuous learning) dapat menjadi strategi efektif untuk menghadapi mutasi serangan siber di masa depan. Ketiga, sistem ini dapat diintegrasikan dengan platform SIEM (Security Information and Event Management) untuk mempercepat respons terhadap serangan aktual secara real-time. Untuk penelitian selanjutnya, disarankan penggunaan arsitektur yang lebih mutakhir seperti Graph Neural Network (GNN) atau Transformer-based IDS untuk meningkatkan sensitivitas terhadap hubungan antar-node dalam jaringan. Selain itu, penggunaan dataset yang lebih realistis seperti CIC-IDS 2021 atau data langsung dari lingkungan jaringan industri (ICS/SCADA, IoT, 5G network) akan meningkatkan validitas eksternal dari model. Peneliti juga dapat menerapkan teknik explainable AI (XAI) agar hasil deteksi sistem menjadi lebih transparan dan mudah dipahami oleh administrator jaringan.

VI. KESIMPULAN

Penelitian ini membuktikan bahwa sistem deteksi intrusi berbasis deep learning mampu memberikan peningkatan signifikan dalam mendeteksi serangan zero-day pada jaringan komputer. Dengan mengimplementasikan model CNN, RNN, dan LSTM, akurasi deteksi mencapai lebih dari 98%, jauh melebihi performa pendekatan konvensional seperti IDS berbasis tanda tangan (signature-based) atau aturan (rule-based). Hasil ini menjawab tujuan utama penelitian, yakni merancang sistem yang mampu mengenali pola serangan baru yang belum terdokumentasi dalam basis data ancaman, sekaligus memberikan respons mitigasi yang cepat dan adaptif. Kontribusi utama dari penelitian ini meliputi tiga aspek. Pertama, pengembangan arsitektur IDS berbasis deep learning yang tidak hanya belajar dari data historis, tetapi mampu menggeneralisasi ke pola serangan baru. Kedua, penggunaan kombinasi fitur statistik dan perilaku jaringan untuk meningkatkan sensitivitas terhadap aktivitas anomali. Ketiga, penyediaan sistem evaluasi komprehensif menggunakan metrik seperti akurasi, precision, recall, dan F1-score sehingga validitas hasil dapat dipertanggungjawabkan secara ilmiah.

Meskipun hasil yang diperoleh sangat menjanjikan, penelitian ini memiliki beberapa keterbatasan. Sistem belum diuji secara langsung pada jaringan berskala besar dengan lalu lintas real-time yang kompleks, sehingga performa di lingkungan produksi masih perlu divalidasi lebih lanjut. Selain itu, konsumsi sumber daya komputasi pada pelatihan model masih relatif tinggi, sehingga memerlukan optimasi agar dapat diterapkan secara efisien pada perangkat dengan sumber daya terbatas. Ke depan, penelitian ini dapat dikembangkan melalui integrasi federated learning untuk memungkinkan pembelajaran terdistribusi tanpa mengorbankan privasi data. Selain itu, penggunaan model hybrid antara deep learning dan reinforcement learning berpotensi menciptakan sistem IDS yang tidak hanya mendeteksi, tetapi juga mampu merespons secara otomatis dan adaptif terhadap pola serangan yang berubah secara dinamis. Implementasi sistem dalam perangkat keras *edge* computing atau network function virtualization (NFV) juga menjadi langkah strategis untuk meningkatkan skalabilitas dan efisiensi. Oleh karena itu, studi ini diharapkan dapat memberikan sumbangsih yang signifikan dalam bidang keamanan jaringan saat ini dengan menyajikan metode deteksi intrusi yang cerdas, fleksibel, dan sesuai untuk menangani ancaman siber di masa mendatang, terutama serangan zero-day yang semakin rumit.

Kontribusi Penulis: Ahmad Farizi bertanggung jawab atas konseptualisasi penelitian, perancangan metodologi, penulisan naskah awal (writing – original draft), penyuntingan naskah (writing – review & editing), serta supervisi keseluruhan proses penelitian. Mohammad Khoirun Nizam berkontribusi dalam pengembangan perangkat lunak (software), pelaksanaan eksperimen dan pengujian sistem (investigation), kurasi dan pengolahan data (data curation), serta turut menulis naskah awal.

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: Tida tersedia
Penulis Pertama: -
Penulis Kedua: -

REFERENSI

[1] F. P. Eka Putra, . S., A. Ramadhani, and . M., "Integrasi Teknologi Kuantum dan fiber Optik untuk Meningkatkan Keamanan dan Efisiensi Jaringan Masa Depan," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 8, no. 2, pp. 151–163, 2025, doi: 10.47324/ilkominfo.v8i2.342.

[2] Y. Singh and T. Walingo, "Smart Water Quality Monitoring with IoT Wireless Sensor Networks," 2024. doi: 10.3390/s24092871.

[3] F. P. E. Putra, U. Ubaidi, R. O. F. Kusuma, A. M. Syam, and S. A. Efendy, "Effect Of Distance On Wi-Fi Signal Quality In The Home Environment," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 391–398, 2024, doi: 10.47709/brilliance.v4i1.4319.

[4] 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.

[5] A. Rachmawardani *et al.*, "Wireless Sensor Network (WSN) of a flood monitoring system based on the Internet of Things (IoT)," 2023. doi: 10.1051/e3sconf/202346401004.

[6] T. T. Nguyen and F. Mohammadi, "Cyber-Physical Power and Energy Systems with Wireless Sensor Networks: A Systematic Review," 2023. doi: 10.1007/s42835-023-01482-3.

[7] A. A. Al-Atawi, "Extending the Energy Efficiency of Nodes in an Internet of Things (IoT) System via Robust Clustering Techniques," 2023. doi: 10.22247/ijcna/2023/223685.

[8] R. Goyal, N. Mittal, L. Gupta, and A. Surana, "Routing Protocols in Wireless Body Area Networks: Architecture, Challenges, and Classification," 2023. doi: 10.1155/2023/9229297.

[9] P. P. Danieli, N. F. Addeo, F. Lazzari, F. Manganello, and F. Bovera, "Precision Beekeeping Systems: State of the Art, Pros and Cons, and Their Application as Tools for Advancing the Beekeeping Sector," 2024. doi: 10.3390/ani14010070.

[10] F. Al-Quayed, Z. Ahmad, and M. Humayun, "A Situation Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0," 2024. doi: 10.1109/ACCESS.2024.3372187.

[11] C. Cao, X. Zhang, C. Song, A. Georgiadis, and G. Goussetis, "A Highly Integrated Multipolarization Wideband Rectenna for Simultaneous Wireless Information and Power Transfer (SWIPT)," 2023. doi: 10.1109/TAP.2023.3306182.

[12] J. Kipongo, T. G. Swart, and E. Esenogho, "Design and Implementation of Intrusion Detection Systems using RPL and AOVD Protocols-based Wireless Sensor Networks," 2023. doi: 10.24425/ijet.2023.144366.

[13] B. Meenakshi and D. Karunkuzhali, "Enhancing cyber security in WSN using optimized self-attention-based provisional variational auto-encoder generative adversarial network," 2024. doi: 10.1016/j.csi.2023.103802.

[14] L. Sahoo, S. S. Sen, K. Tiwary, S. Moslem, and T. Senapati, "Improvement of Wireless Sensor Network Lifetime via Intelligent Clustering Under Uncertainty," 2024. doi: 10.1109/ACCESS.2024.3365490.

[15] M. Alsharif, A. Jahid, A. Kelechi, and R. Kannadasan, "Green IoT: A Review and Future Research Directions," 2023. doi: 10.3390/sym15030757.

[16] A. Khan and I. Sharma, "Leveraging Artificial Intelligence Methodologies to Improve WSN Security," 2023. doi: 10.1109/GCAT59970.2023.10353254.

[17] M. Sajid *et al.*, "Enhancing intrusion detection: a hybrid machine and deep learning approach," 2024. doi: 10.1186/s13677-024-00685-x.

[18] H. Moudoud, Z. A. El Houda, and B. Brik, "Advancing Security and Trust in WSNs: A Federated Multi-Agent Deep Reinforcement Learning Approach," 2024. doi: 10.1109/TCE.2024.3440178.

[19] 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.
[20] F. P. Eka Putra, Amir Hamzah, W. Agel, and R. O. Firmansyah Kusuma, "Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking," *J. Sistim Inf. dan Teknol.*, pp. 82–87, 2024, doi: 10.60083/jsisfotek.v5i4.329.
[21] T. Alahmad, M. Neményi, and A. Nyéki, "Applying IoT Sensors and Big Data to Improve Precision Crop Production: A Review," 2023. doi: 10.3390/agronomy13102603.
[22] M. Devika and S. M. Shaby, "Optimizing Wireless Sensor Networks: A Deep Reinforcement Learning-Assisted Butterfly Optimization Algorithm in MOD-LEACH Routing for Enhanced Energy Efficiency," 2024. doi: 10.22399/ijcesen.708.
[23] R. Alharthi, "Enhancing unmanned aerial vehicle and smart grid communication security using a ConvLSTM model for intrusion detection," 2024. doi: 10.3389/fenrg.2024.1491332.
[24] R. Khan, U. Saeed, and I. Koo, "FedLSTM: A Federated Learning Framework for Sensor Fault Detection in Wireless Sensor Networks," 2024. doi: 10.3390/electronics13244907.
[25] K. Fang, J. Chen, H. Zhu, T. R. Gadekallu, X. Wu, and W. Wang, "Explainable-AI-based two-stage solution for WSN object localization using zero-touch mobile transceivers," 2024. doi: 10.1007/s11432-023-3968-9.
[26] S. Qin and X. Guo, "IoT Edge-Computing-Enabled Efficient Localization via Robust Optimal Estimation," 2023. doi: 10.1109/JIOT.2022.3200095.
[27] R. Anwit, P. K. Jana, and M. S. Obaidat, "Obstacle Adaptive Smooth Path Planning for Mobile Data Collector in the Internet of Things," 2023. doi: 10.1109/TSUSC.2023.3281886.
[28] S. Madhavi, N. C. Santhosh, S. Rajkumar, and R. Praveen, "Pythagorean Fuzzy Sets-based VIKOR and TOPSIS-based multi-criteria decision-making model for mitigating resource deletion attacks in WSNs," 2023. doi: 10.3233/jifs-224141.
[29] F. P. Eka Putra, L. Fitriyah, Z. Naimah, and S. A. Rofika, "Evaluasi Kinerja Aplikasi Wireshark Dalam Monitoring Jaringan Kecil Dengan Topologi Star dan Bus," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 8, no. 2, pp. 164–176, 2025, doi: 10.47324/ilkominfo.v8i2.343.
[30] M. Matar, T. Xia, K. D. Huguenard, D. Huston, and S. Wshah, "Anomaly Detection in Coastal Wireless Sensors via Efficient Deep Sequential Learning," 2023. doi: 10.1109/ACCESS.2023.3322370.
[31] A. F. Rachman, F. P. E. Putra, S. Syirofi, and D. Wahid, "Case Study of Computer Network Development for the Internet Of Things (IoT) Industry in an Urban Environment," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 399–407, 2024, doi: 10.47709/brilliance.v4i1.4302.
[32] P. Wasnik and N. Chavhan, "A Review Paper on Designing Intelligent Intrusion Detection System Using Deep Learning," 2023. doi: 10.1109/ICETET-SIP58143.2023.10151563.
[33] F. P. Eka Putra, A. Muzayyin, and M. U. Mansyur, "ANALISIS KUALITAS LAYANAN ABSENSI BERBASIS FINGER BERDASARKAN Quality of Service," *J. Inform.*, vol. 24, no. 1, pp. 17–25, 2024, doi: 10.30873/ji.v24i1.3949.
[34] 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.
[35] M. Matar, T. Xia, K. D. Huguenard, D. Huston, and S. Wshah, "Multi-Head Attention based Bi-LSTM for Anomaly Detection in Multivariate Time-Series of WSN," 2023. doi: 10.1109/AICAS57966.2023.10168670.
[36] R. Amutha, G. G. Sivasankari, and K. R. Venugopal, "Node clustering and data aggregation in wireless sensor network using sailfish optimization," 2023. doi: 10.1007/s11042-023-15225-z.
[37] 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.
[38] M. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, and S. Aryal, "MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs," 2024. doi: 10.1007/s10207-024-00833-z.
[39] H. Kang, J. Yoon, S. R. H. Madjid, S. J. Hwang, and C. D. Yoo, "Forget-free Continual Learning with Soft-Winning SubNetworks," 2023. doi: 10.48550/arXiv.2303.14962.
[40] F. P. E. Putra, D. A. M. Putra, A. Firdaus, and A. Hamzah, "Analisis Kecepatan Dan Kinerja Jaringan 5G (generasi ke 5) Pada Wilayah Perkotaan," *INFORMATICS Educ. Prof. J. Informatics*, vol. 8, no. 1, p. 47, 2023, doi: 10.51211/itbi.v8i1.2439.
[41] N. Yang *et al.*, "A Blade-Type Triboelectric-Electromagnetic Hybrid Generator with Double Frequency Up-Conversion Mechanism for Harvesting Breeze Wind Energy," 2024. doi: 10.1021/acsami.4c04377.
[42] N. Vidhya and C. Meenakshi, "Blockchain-Enabled Secure Data Aggregation Routing (BSDAR) Protocol for IoT-Integrated Next-Generation Sensor Networks for Enhanced Security," 2025. doi: 10.22399/ijcesen.722.

[43] Y. Bai, B. Xie, R. Zhu, Z. Chang, and R. Jäntti, "Movable Antenna-Equipped UAV for Data Collection in Backscatter Sensor Networks: A Deep Reinforcement Learning-Based Approach," 2024. doi: 10.1109/ICC52391.2025.11162069.

[44] R. F. Miranda *et al.*, "A Review of Cognitive Hybrid Radio Frequency/Visible Light Communication Systems for Wireless Sensor Networks," 2023. doi: 10.3390/s23187815.

[45] B. Al-Fuhaidi, Z. Farae, F. Al-Fahaidy, G. Nagi, A. Ghallab, and A. Alameri, "Anomaly-Based Intrusion Detection System in Wireless Sensor Networks Using Machine Learning Algorithms," 2024. doi: 10.1155/2024/2625922.

[46] N. Dharini, J. Katiravan, S. D. M. Priya, and S. V. A. Sneghaa, "Intrusion Detection in Novel WSN-Leach Dos Attack Dataset using Machine Learning based Boosting Algorithms," 2023. doi: 10.1016/j.procs.2023.12.064.

[47] A. Oztoprak, R. Hassanpour, A. Ozkan, and K. Oztoprak, "Security Challenges, Mitigation Strategies, and Future Trends in Wireless Sensor Networks: A Review," 2024. doi: 10.1145/3706583.

[48] R. Arunachalam and E. D. R. Kanmani, "Detection and mitigation of vampire attacks with secure routing in WSN using weighted RNN and optimal path selection," 2024. doi: 10.1016/j.cose.2024.103991.

[49] S. Madhavi, S. M. Udhaya Sankar, R. Praveen, and N. Jagadish Kumar, "A fuzzy COPRAS-based decision-making framework for mitigating the impact of vampire sensor nodes in wireless sensor nodes (WSNs)," 2023. doi: 10.1007/s41870-023-01219-5.

[50] B. Prince, P. Kumar, and S. K. Singh, "Multi-level clustering and Prediction based energy efficient routing protocol to eliminate Hotspot problem in Wireless Sensor Networks.," 2025. doi: 10.1038/s41598-024-84596-6.