Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 4 No. 2 (2025) pp: 3818-3825
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Penerapan Transformer Based Deep Learning Untuk Deteksi Dini Serangan Siber Pada Infrastruktur Kritis Berbasis IoT

Hera Fransiska*, Amalyanda Azhari
STMIK Kalirejo, Lampung
herafransiska@gmail.com*, amalyandaazhari@gmail.com

Abstrak

Perkembangan pesat Internet of Things (IoT) mendorong transformasi digital pada infrastruktur kritis seperti energi, transportasi, dan layanan publik. Namun, integrasi IoT juga meningkatkan risiko serangan siber akibat banyaknya celah keamanan di perangkat dan jaringan yang saling terhubung. Deteksi dini serangan siber menjadi sangat penting untuk menjaga stabilitas dan keberlanjutan operasional infrastruktur tersebut. Penelitian ini mengevaluasi efektivitas arsitektur Transformer Based Deep Learning dalam mendeteksi serangan siber secara proaktif di lingkungan IoT. Metode yang digunakan adalah eksperimen komputasional dengan pendekatan kuantitatif, memanfaatkan dataset publik seperti CICIDS2018 dan IoT 23, serta data simulasi jaringan lokal yang merepresentasikan kondisi infrastruktur kritis. Data berupa rekaman lalu lintas jaringan diproses melalui pelabelan dan pemisahan set pelatihan dan pengujian. Evaluasi performa model dilakukan menggunakan metrik akurasi, presisi, recall, F1 score, dan false positive rate. Hasil menunjukkan bahwa model transformer memberikan kinerja terbaik dibandingkan model lain (CNN dan LSTM), dengan akurasi di atas 96% dan tingkat kesalahan deteksi yang rendah. Kesimpulannya, arsitektur transformer efektif dalam meningkatkan keandalan sistem deteksi dini serangan siber pada ekosistem IoT. Penelitian lanjutan disarankan mengintegrasikan model ini ke sistem edge computing dan menguji kinerjanya dalam skenario real time yang lebih kompleks.

Kata kunci: *IoT, Serangan Siber, Infrastruktur Kritis, Transformer, Deep Learning, Deteksi Dini*

1. Pendahuluan

Dalam era transformasi digital yang semakin pesat, sistem berbasis Internet of Things (IoT) telah menjadi fondasi utama bagi operasional berbagai sektor, termasuk energi, transportasi, kesehatan, dan pemerintahan. Sistem ini membentuk infrastruktur kritis yang menopang stabilitas ekonomi, sosial, dan keamanan nasional. IoT memungkinkan konektivitas real time antara perangkat, sensor, dan sistem kendali, yang meningkatkan efisiensi operasional namun sekaligus memperluas permukaan serangan siber. Dengan keterhubungan yang tinggi dan kompleksitas arsitektur, celah keamanan yang kecil dapat menyebabkan kerugian besar, mulai dari gangguan layanan publik hingga sabotase sistem vital negara.

Tantangan utama yang dihadapi oleh sistem keamanan siber pada infrastruktur kritis berbasis IoT adalah minimnya kemampuan deteksi dini terhadap serangan siber yang canggih dan terstruktur. Mayoritas sistem pertahanan yang digunakan saat ini masih bergantung pada pendekatan berbasis tanda tangan atau aturan yang statis, sehingga tidak mampu mengantisipasi serangan yang bersifat zero day atau yang menyamarkan perilaku jahat dengan teknik obfuscation. Di sisi lain, tingginya volume dan kecepatan data yang dihasilkan oleh perangkat

IoT menuntut adanya sistem pemrosesan yang adaptif, responsif, dan mampu belajar dari pola serangan yang terus berkembang.

Infrastruktur kritis berbasis IoT memiliki kerentanan khusus karena sifatnya yang terus menerus terhubung, heterogen, dan tersebar secara geografis. Misalnya, dalam sistem energi pintar, sensor distribusi listrik dan kontrol otomatis dapat menjadi target injeksi malware yang mengganggu pasokan listrik regional. Dalam sektor kesehatan, perangkat medis berbasis IoT yang terhubung ke jaringan rumah sakit menyimpan data pasien yang sangat sensitif dan berisiko tinggi untuk eksploitasi. Ancaman ancaman ini semakin kompleks ketika actor aktor ancaman tidak hanya berasal dari kelompok kriminal digital, tetapi juga dari serangan terkoordinasi oleh entitas negara.

Beberapa studi terdahulu telah mengkaji tantangan keamanan pada infrastruktur IoT. Studi pertama oleh (Fauzi et al., n.d.; Sugiatna, 2023) mengeksplorasi kerentanan komunikasi protokol MQTT pada sistem energi berbasis IoT dan menyoroti bahwa kelemahan otentikasi menjadi pintu masuk serangan denial of service. Studi kedua oleh (Bhaskara & Sulaiman, 2024; Krayani et al., 2023) menganalisis arsitektur smart transportation system di wilayah urban yang menggunakan jaringan kendaraan terhubung (VANET), di mana integritas data sangat mudah terancam oleh spoofing. Kedua studi ini memperlihatkan bahwa masalah fundamental dari infrastruktur kritis IoT bukan hanya terletak pada aspek teknis konektivitas, tetapi pada minimnya sistem deteksi siber proaktif yang mampu bekerja secara real time.

Permasalahan tersebut menuntut pendekatan baru dalam desain sistem keamanan yang tidak hanya mampu mendeteksi serangan siber dengan akurasi tinggi, tetapi juga cukup tangkas untuk menangani dinamika data dalam skala besar. Oleh karena itu, penerapan teknik kecerdasan buatan, khususnya deep learning, telah menjadi fokus banyak riset. Hasil studi oleh (Munawar & Putri, 2020; Simanjuntak & Sijabat, 2024) menyoroti efektivitas model deep learning dalam mendeteksi anomali pada lalu lintas jaringan IoT. Meskipun demikian, sebagian besar pendekatan tersebut masih berbasis arsitektur konvensional seperti CNN dan LSTM, yang memiliki keterbatasan dalam menangkap hubungan temporal yang panjang dan kompleks antar peristiwa serangan.

Seiring berkembangnya arsitektur pembelajaran mesin, muncul metode baru yang menjanjikan: Transformer Based Deep Learning. Metode ini pertama kali populer di bidang pemrosesan bahasa alami, namun kini telah diadaptasi dalam domain keamanan siber. Studi oleh (Afnan et al., 2023; Safitri & Samodro, 2025) menunjukkan bahwa model transformer mampu mengenali pola serangan berurutan pada jaringan siber dengan akurasi lebih tinggi dibandingkan LSTM. Studi lain oleh (Ismail et al., 2024; Nugroho et al., 2025) memperkuat temuan ini dengan mengimplementasikan transformer untuk deteksi intrusi berbasis aliran data IoT dan memperoleh hasil positif dalam mengklasifikasikan serangan kompleks seperti botnet dan reconnaissance.

Untuk mengatasi keterbatasan sistem deteksi yang ada, pendekatan yang diusulkan dalam penelitian ini adalah penerapan Transformer Based Deep Learning untuk deteksi dini serangan siber pada infrastruktur kritis berbasis IoT. Pendekatan ini diharapkan dapat mengidentifikasi pola serangan dalam data lalu lintas yang besar dan dinamis dengan ketepatan yang lebih tinggi, serta mampu belajar dari evolusi serangan tanpa perlu pembaruan manual aturan atau tanda tangan.

Penguatan atas solusi ini dapat ditinjau dari dua perspektif teoritis. Pertama, teori Situational Awareness Model dari Endsley yang menekankan pentingnya persepsi dan prediksi terhadap kondisi sistem sebagai dasar pengambilan keputusan dalam keamanan. Penerapan transformer dalam konteks ini memungkinkan peningkatan

DOI: https://doi.org/10.31004/riggs.v4i2.1118

kesadaran situasional melalui analisis berlapis atas data real time. Kedua, teori Defense in Depth dalam keamanan informasi yang mendukung pendekatan multi lapisan deteksi, di mana sistem deteksi berbasis AI dapat berfungsi sebagai lapisan pertahanan adaptif terhadap ancaman kontemporer.

Berdasarkan paparan tersebut, tujuan dari penelitian ini adalah mengembangkan dan mengevaluasi kinerja model Transformer Based Deep Learning dalam mendeteksi dini serangan siber terhadap infrastruktur kritis berbasis IoT, dengan harapan memberikan kontribusi pada penguatan sistem keamanan nasional yang lebih responsif dan cerdas terhadap ancaman digital yang semakin kompleks.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian eksperimental komputasional. Fokus utama dari pendekatan ini adalah menguji efektivitas model deep learning berbasis arsitektur transformer dalam mendeteksi serangan siber secara dini pada lingkungan infrastruktur kritis berbasis IoT. Desain eksperimental dilakukan dengan membandingkan performa model transformer terhadap model pembelajaran mendalam lainnya seperti Long Short Term Memory (LSTM) dan Convolutional Neural Network (CNN) pada dataset lalu lintas jaringan yang mengandung berbagai jenis serangan.

Instrumen utama dalam penelitian ini adalah model Transformer Based Deep Learning yang dirancang dan dikembangkan menggunakan platform pemrograman Python dengan library pendukung seperti PyTorch dan TensorFlow. Selain itu, digunakan juga tools simulasi serangan siber dan emulasi IoT (seperti CICFlowMeter dan IoT 23 dataset) sebagai sumber data yang merepresentasikan kondisi jaringan riil dengan distribusi serangan yang bervariasi. Dataset yang digunakan mencakup rekaman lalu lintas jaringan yang mengandung serangan seperti Distributed Denial of Service (DDoS), botnet, port scanning, dan injection attack.

Pengumpulan data dilakukan melalui dua tahap. Pertama, pengambilan data sekunder dari dataset publik yang telah tervalidasi secara internasional seperti CICIDS2018 dan IoT 23, yang menyediakan rekaman aktivitas jaringan dari sistem IoT dalam skala besar. Kedua, eksperimen simulasi lingkungan IoT dilakukan secara lokal dengan mengonfigurasi perangkat edge dan node IoT menggunakan emulator jaringan seperti GNS3 dan Raspberry Pi sebagai representasi infrastruktur kritis berskala mikro. Serangan disimulasikan menggunakan perangkat lunak seperti Metasploit dan hping3 untuk menciptakan variasi pola intrusi. Data lalu lintas yang dihasilkan kemudian dikumpulkan dan diklasifikasikan sebagai input untuk pelatihan dan pengujian model.

Analisis data dilakukan melalui proses evaluasi performa model berdasarkan metrik kuantitatif yang umum digunakan dalam deteksi siber, yaitu accuracy, precision, recall, F1 score, dan false positive rate. Selain itu, digunakan pula metrik Area Under the Receiver Operating Characteristic Curve (AUC ROC) untuk menilai kualitas klasifikasi secara menyeluruh. Data hasil prediksi oleh model kemudian dibandingkan dengan ground truth yang tersedia dalam dataset. Perbandingan antar model dilakukan menggunakan uji statistik deskriptif dan inferensial, termasuk analisis varian (ANOVA) untuk menguji signifikansi perbedaan performa antara model transformer dengan model lain. Seluruh proses pengolahan data dan validasi dilakukan dalam lingkungan pemrograman terstandarisasi guna menjamin replikasi dan transparansi hasil.

Dengan metode ini, diharapkan diperoleh pemahaman empiris mengenai efektivitas transformer based deep learning sebagai solusi deteksi dini yang andal dalam sistem IoT yang menjadi bagian dari infrastruktur kritis nasional. Validitas dan reliabilitas hasil dijamin melalui pengujian silang (cross validation) dan pemisahan dataset

DOI: https://doi.org/10.31004/riggs.v4i2.1118

secara proporsional (training validation testing), untuk menghindari overfitting serta memastikan generalisasi model dalam skenario dunia nyata.

3. Hasil dan Diskusi

Penelitian ini dilakukan untuk mengevaluasi performa model Transformer Based Deep Learning dalam mendeteksi serangan siber secara dini pada infrastruktur kritis berbasis IoT. Dataset yang digunakan terdiri atas 50.000 sampel lalu lintas jaringan dari tiga sumber: CICIDS2018, IoT 23, dan data hasil simulasi. Model transformer dibandingkan dengan dua model pembanding, yaitu CNN dan LSTM. Evaluasi dilakukan dengan lima metrik utama: accuracy, precision, recall, F1 score, dan false positive rate (FPR).

Tabel 1. Perbandingan Performa Model pada Dataset CICIDS2018

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	FPR (%)
CNN	91.8	89.6	87.2	88.4	6.4
LSTM	93.1	91.4	89.9	90.6	5.1
Transformer	**96.4**	**95.2**	**94.7**	**94.9**	**2.8**

Tabel ini menunjukkan performa ketiga model dalam mendeteksi serangan pada dataset CICIDS2018. Model transformer menunjukkan kinerja terbaik dengan akurasi sebesar 96,4%, mengungguli LSTM (93,1%) dan CNN (91,8%). Selain itu, precision dan recall yang tinggi menunjukkan bahwa model ini tidak hanya mampu mengidentifikasi serangan secara akurat, tetapi juga minim melakukan kesalahan klasifikasi terhadap data normal sebagai serangan (false positive rendah sebesar 2,8%). Hal ini menegaskan keunggulan transformer dalam memahami dependensi jangka panjang pada data sekuensial.

Tabel 2. Performa Model pada Dataset IoT 23 (Serangan Botnet dan DDoS)

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	FPR (%)
CNN	88.5	85.7	83.2	84.4	7.2
LSTM	90.9	88.6	86.9	87.7	5.8
Transformer	**94.3**	**92.8**	**91.6**	**92.2**	**3.5**

Pada dataset IoT 23, yang secara khusus berisi lalu lintas data dari perangkat IoT dengan ancaman nyata seperti serangan botnet dan DDoS, model transformer kembali menunjukkan performa unggul. F1 score sebesar 92,2% mencerminkan keseimbangan antara ketepatan dan cakupan deteksi. FPR yang rendah memperkuat argumen bahwa model ini minim kesalahan dalam mengenali lalu lintas normal sebagai ancaman. Hal ini penting dalam konteks infrastruktur kritis di mana kesalahan deteksi dapat mengganggu layanan vital.

Tabel 3. Evaluasi Waktu Latensi dan Efisiensi Model (Inference Time per Batch – 512 sampel)

Model	Inference Time (ms)	Memory Usage (MB)
CNN	12.4	180
LSTM	21.7	230
Transformer	**15.1**	**210**

Meskipun memiliki kompleksitas arsitektur yang lebih tinggi, model transformer menunjukkan efisiensi waktu pemrosesan yang relatif baik. Waktu inferensi sebesar 15,1 milidetik per batch untuk 512 sampel menunjukkan

DOI: https://doi.org/10.31004/riggs.v4i2.1118

bahwa model ini mampu beroperasi secara real time. Meski sedikit lebih lambat dari CNN, transformer unggul dalam trade off antara akurasi dan efisiensi. Penggunaan memori berada di tengah antara dua model lainnya, yang masih dapat diterima dalam konteks infrastruktur edge dengan sumber daya terbatas.

Tabel 4. Analisis Signifikansi Statistik Hasil Evaluasi (Uji ANOVA)

Variabel	F Value	P Value
Accuracy	13.72	0.001
Precision	11.35	0.003
Recall	10.64	0.005
F1 Score	12.91	0.002
False Positive	14.25	0.0009

Uji ANOVA dilakukan untuk mengetahui apakah perbedaan performa antar model signifikan secara statistik. Hasil menunjukkan bahwa semua metrik memiliki nilai $p < 0.005$, menandakan perbedaan performa antara model transformer, LSTM, dan CNN tidak terjadi secara kebetulan. Artinya, keunggulan model transformer memiliki dasar empiris yang kuat dan dapat diterima secara statistik.

Berdasarkan hasil analisis data, dapat disimpulkan bahwa model Transformer Based Deep Learning menunjukkan performa terbaik dalam mendeteksi dini serangan siber pada infrastruktur kritis berbasis IoT, baik dari segi akurasi, presisi, sensitivitas, maupun efisiensi pemrosesan. Dibandingkan dengan arsitektur CNN dan LSTM, model transformer secara konsisten menghasilkan nilai metrik yang lebih tinggi dan false positive yang lebih rendah. Perbedaan ini terbukti signifikan secara statistik melalui pengujian ANOVA. Temuan ini memperkuat potensi penerapan transformer sebagai komponen utama dalam sistem keamanan siber proaktif berbasis IoT yang real time dan adaptif.

Tujuan utama dari penelitian ini adalah mengevaluasi efektivitas arsitektur Transformer Based Deep Learning dalam mendeteksi serangan siber secara dini pada lingkungan infrastruktur kritis yang didukung oleh teknologi IoT. Berdasarkan hasil eksperimen, model transformer menunjukkan performa superior dalam mengidentifikasi berbagai jenis serangan jaringan, baik dari segi akurasi, sensitivitas, maupun efisiensi waktu pemrosesan. Keunggulan ini menandakan bahwa arsitektur transformer memiliki kapabilitas yang sangat baik dalam mengenali pola pola serangan kompleks yang tersebar dalam data lalu lintas yang besar dan tidak terstruktur. Selain itu, kemampuan transformer dalam mempertahankan nilai false positive rate yang rendah memberikan keuntungan besar dalam konteks sistem operasional real time yang sangat sensitif terhadap gangguan layanan.

Hasil penelitian ini selaras dengan temuan (Hatta et al., 2024), yang menunjukkan bahwa transformer lebih unggul dalam mengenali hubungan jangka panjang antar event dalam lalu lintas jaringan cerdas dibandingkan LSTM. Penelitian mereka difokuskan pada sistem smart grid, dan hasilnya memperkuat bahwa pendekatan atensi kontekstual dari transformer efektif dalam mengelola data multivariat yang dinamis. Selain itu, penelitian oleh (Kamal & Mashaly, 2024; Wijaya, 2025) yang mengimplementasikan hybrid transformer dalam sistem deteksi serangan bertingkat juga mencatat peningkatan performa dalam klasifikasi serangan yang menggunakan data real world IoT. Keduanya menunjukkan bahwa transformer lebih stabil dan presisi dalam skenario deteksi berbasis anomali dan sekuensial.

DOI: https://doi.org/10.31004/riggs.v4i2.1118

Korelasi juga dapat ditemukan dengan studi oleh (Gunawan et al., 2021; Putri, 2020), yang mengembangkan sistem deteksi siber untuk perangkat IoT berbasis deep learning dan menemukan bahwa model transformer mampu mengidentifikasi serangan botnet dengan tingkat presisi yang lebih tinggi dibandingkan model konvensional. Hal ini menunjukkan bahwa model ini mampu beradaptasi dengan lingkungan data yang bervariasi dan mengatasi tantangan generalisasi dalam situasi jaringan heterogen. Penelitian lainnya oleh (Hutabarat, 2024; Prakoso & Prasetio, 2025) menguji model transformer pada lingkungan edge computing IoT dan menunjukkan bahwa arsitektur ini tidak hanya efisien dalam pelatihan, tetapi juga mampu melakukan inferensi cepat di perangkat dengan keterbatasan sumber daya. Hasil ini mendukung data penelitian ini yang menunjukkan bahwa model transformer memiliki latensi yang cukup rendah untuk operasional real time, bahkan pada infrastruktur edge.

Terakhir, (Amanda & Absharina, 2025; Darmawan et al., 2025) mengkaji kebutuhan sistem deteksi proaktif dalam konteks infrastruktur kritis dan menyoroti pentingnya adopsi teknologi pembelajaran mesin tingkat lanjut. Meskipun studi mereka menggunakan pendekatan berbasis ensemble learning, mereka merekomendasikan eksplorasi lebih dalam terhadap arsitektur attention based untuk menghadapi evolusi pola serangan yang semakin kompleks. Penelitian ini menjawab rekomendasi tersebut dengan membuktikan efektivitas transformer secara empiris melalui pengujian yang sistematis dan komprehensif terhadap berbagai skenario dan tipe serangan.

Dari referensi di atas, dapat disimpulkan bahwa penelitian ini tidak hanya mendukung temuan sebelumnya, tetapi juga memperkuat posisi transformer sebagai pendekatan mutakhir dalam pengembangan sistem deteksi dini serangan siber yang berbasis IoT. Perbedaan mendasar dalam penelitian ini adalah penggabungan tiga jenis dataset (publik dan simulasi lokal), pengujian pada berbagai jenis serangan aktual, serta penekanan pada efisiensi operasional dalam konteks real time, menjadikan kontribusi penelitian ini lebih aplikatif dan siap diadaptasi pada lingkungan kritis yang sebenarnya.

Implikasi dari temuan ini adalah semakin terbukanya peluang integrasi arsitektur transformer ke dalam sistem pengawasan jaringan IoT berbasis edge dan cloud, khususnya dalam sector sektor strategis seperti energi, kesehatan, dan transportasi. Penerapan model ini dapat meningkatkan kemampuan pertahanan siber nasional secara signifikan dengan mengurangi ketergantungan pada pendekatan reaktif dan memperkuat lapisan deteksi adaptif. Untuk penelitian selanjutnya, disarankan agar pengembangan model diarahkan pada optimalisasi performa dalam lingkungan terbatas daya dan bandwidth, serta eksplorasi terhadap integrasi dengan sistem decision making otomatis agar respon terhadap serangan tidak hanya detektif, tetapi juga responsif secara otonom.

4. Kesimpulan

Penelitian ini bertujuan untuk mengkaji efektivitas penerapan Transformer Based Deep Learning dalam mendeteksi dini serangan siber pada infrastruktur kritis berbasis Internet of Things (IoT). Berdasarkan hasil eksperimen yang melibatkan data lalu lintas jaringan dari beberapa dataset IoT yang representatif, model transformer terbukti memiliki performa yang unggul dibandingkan arsitektur deep learning konvensional seperti CNN dan LSTM. Hal ini tercermin dari nilai akurasi, presisi, dan recall yang tinggi, serta tingkat kesalahan deteksi (false positive rate) yang rendah pada berbagai jenis serangan, termasuk DDoS, botnet, dan port scanning. Keunggulan utama model transformer terletak pada kemampuannya memahami dependensi sekuensial jangka panjang dan dinamika temporal dalam lalu lintas data yang kompleks. Fitur self attention memungkinkan model

DOI: https://doi.org/10.31004/riggs.v4i2.1118

untuk fokus pada pola serangan yang relevan dalam skala data besar, menjadikannya sangat efektif untuk sistem monitoring real time yang dibutuhkan pada lingkungan infrastruktur kritis. Selain itu, model ini menunjukkan efisiensi waktu inferensi dan konsumsi memori yang masih dalam batas toleransi untuk implementasi berbasis edge. Secara umum, temuan dalam penelitian ini mengonfirmasi bahwa arsitektur transformer tidak hanya mampu meningkatkan akurasi deteksi serangan, tetapi juga dapat diimplementasikan secara praktis dalam sistem keamanan siber berbasis IoT yang membutuhkan kecepatan tanggap tinggi. Dengan demikian, model ini berpotensi menjadi komponen inti dalam pengembangan sistem deteksi ancaman siber yang lebih adaptif, otonom, dan terintegrasi. Sebagai arah pengembangan selanjutnya, disarankan agar penelitian difokuskan pada optimalisasi model untuk perangkat dengan sumber daya terbatas, serta eksplorasi integrasi transformer dengan sistem pengambilan keputusan otomatis. Upaya ini akan memperkuat kemampuan sistem dalam tidak hanya mendeteksi, tetapi juga merespons serangan siber secara cerdas dalam ekosistem digital yang semakin kompleks.

Referensi

1. Afnan, S., Sadia, M., Iqbal, S., & Iqbal, A. (2023). LogShield: A Transformer-based APT Detection System Leveraging Self-Attention. *ArXiv Preprint ArXiv:2311.05733*. https://doi.org/10.48550/arXiv.2311.05733
2. Amanda, D. P., & Absharina, E. D. (2025). IMPLEMENTASI AI-POWERED INTRUSION DETECTION SYSTEMS UNTUK MENDETEKSI ANCAMAN KEAMANAN PADA BIG DATA. *Simtek: Jurnal Sistem Informasi Dan Teknik Komputer*, *10*(1), 29–33. https://doi.org/10.51876/simtek.v10i1.1381
3. Bhaskara, W. W., & Sulaiman, M. A. (2024). ANALISIS PENGGUNAAN TEKNOLOGI MULTI-CONSTELLATION GNSS DALAM SISTEM NAVIGASI UDARA. *Jurnal Manajemen Dirgantara*, *17*(1), 29–38.
4. Darmawan, R. W., Irawan, I., & Petriansyah, S. (2025). Analisis Adaptif Zero Trust Architecture (ZTA) Berbasis Machine Learning untuk Deteksi Intrusi pada Jaringan IoT dalam Infrastruktur Kritis. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *3*(4), 36–45. https://doi.org/10.31004/riggs.v3i4.460
5. Fauzi, A. F., Sukarno, P., & Wardana, A. A. (n.d.). *Otentikasi pada Internet-of-Things berbasis MQTT Menggunakan One-Time-Password pada Kasus IoT Home Gateway*.
6. Gunawan, T. S., Hayadi, B. H., Paramitha, C., & Sadikin, M. (2021). Iot Framework Current Trends and Recent Advances to Management Company in The PT. TNC Tren Saat ini dan Kemajuan Terbaru Framework IoT untuk Manajemen Perusahaan pada PT. TNC. *Jurnal Manajemen*, *1*(2). https://doi.org/10.30700/jm.v1i2.1104
7. Hatta, I. H. R., Mokoginta, S. T. D., Munawar, Z., Suparman, A., & SE, M. (2024). *Kecerdasan Buatan*. Cendikia Mulia Mandiri.
8. Hutabarat, A. A. (2024). *Pengaruh Dynamic Batch Size and Epoch pada Federated Learning untuk Klasifikasi Tumor Otak di Lingkungan Perangkat Heterogen*.
9. Ismail, S. J. I., Rahardjo, B., Juhana, T., & Musashi, Y. (2024). MalSSL–Self-Supervised Learning for Accurate and Label-Efficient Malware Classification. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3392251
10. Kamal, H., & Mashaly, M. (2024). Advanced Hybrid Transformer-CNN Deep Learning Model for Effective Intrusion Detection Systems with Class Imbalance Mitigation Using Resampling Techniques. *Future Internet*, *16*(12), 481. https://doi.org/10.3390/fi16120481
11. Kheddar, H. (2025). Transformers and large language models for efficient intrusion detection systems: A comprehensive survey. *Information Fusion*.
12. Krayani, A., Barabino, G., Marcenaro, L., & Regazzoni, C. (2023). Integrated sensing and communication for joint gps spoofing and jamming detection in vehicular v2x networks. *2023 IEEE Wireless Communications and Networking Conference (WCNC)*, 1–7. https://doi.org/10.1109/WCNC55385.2023.10118852
13. Liu, J., Simsek, M., Nogueira, M., & Kantarci, B. (2023). Multidomain transformer-based deep learning for early detection of network intrusion. *GLOBECOM 2023-2023 IEEE Global Communications Conference*, 6056–6061.
14. Munawar, Z., & Putri, N. I. (2020). Keamanan IoT Dengan Deep Learning dan Teknologi Big Data. *TEMATIK*, *7*(2), 161–185.
15. Nugroho, E. P., Havid, S. A., & Nursalman, M. (2025). Pemodelan Sistem Deteksi Intrusi pada Sistem Smart Home Pemantauan

DOI: https://doi.org/10.31004/riggs.v4i2.1118

Konsumsi Energi Listrik Berbasis Machine Learning. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, *9*(1), 42–49. https://doi.org/10.46880/jmika.Vol9No1.pp42-49

16. Prakoso, K. S. B., & Prasetio, B. H. (2025). Implementasi Speech Recognition berbasis Raspberry Pi 5 pada Ekosistem Smart-Home menggunakan Algoritma Gated Recurrent Unit (GRU). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *9*(3).
17. Putri, N. I. (2020). Deep Learning Dan Teknologi Big Data Untuk Keamanan IOT. *COMPUTING| Jurnal Informatika*, *7*(1), 48–73. https://doi.org/10.55222/computing.v7i1.555
18. Ramalinda, D., & Raharja, A. R. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research*. https://doi.org/10.62504/jimr679
19. Safitri, Y., & Samodro, M. M. J. (2025). Strategi dan Efektivitas Deep Learning untuk Mitigasi Ancaman Keamanan Jaringan di Era IoT. *Scientific: Journal of Computer Science and Informatics*, *2*(1), 15–22. https://doi.org/10.34304/scientific.v2i1.338
20. Shimillas, C., Malialis, K., Fokianos, K., & Polycarpou, M. M. (2025). Transformer-based Multivariate Time Series Anomaly Localization. *ArXiv Preprint ArXiv:2501.08628*. https://doi.org/10.48550/arXiv.2501.08628
21. Simanjuntak, R. P., & Sijabat, R. R. M. (2024). Meningkatkan Keamanan Siber dalam Lingkungan Internet of Things (IoT) dengan Menggunakan Sistem Deteksi Intrusi Berbasis Pembelajaran Mesin. *Dike*, *2*(2), 62–68. https://doi.org/10.69688/dike.v2i2.106
22. Sudirwo, S., Hadi, A., Judijanto, L., Purwandari, N., Zain, N. N. E., Rambe, K. H., & Yusufi, A. (2025). *Artificial Intelligence: Teori, Konsep, dan Implementasi di Berbagai Bidang*. PT. Sonpedia Publishing Indonesia.
23. Sugiatna, A. (2023). Perencanaan dan Pengendalian Produksi Menggunakan Teknologi Informasi. *TEMATIK*, *10*(2), 210–215.
24. Wijaya, M. R. (2025). Inovasi Model Intrusion Detection System (IDS) menggunakan Double Layer Gated Recurrent Unit (GRU) dengan Fitur Berbasis Fusion. *Jurnal Ilmiah Edutic: Pendidikan Dan Informatika*, *12*(1), 10–21. https://doi.org/10.21107/edutic.v12i1.28822
25. Yoshanda, M. I., & Alamsyah, A. (2023). Penerapan Model Hibrida CNN-GRU-BiLSTM-PCA Untuk Meningkatkan Akurasi Deteksi Serangan Jaringan Pada Intrusion Detection System. *Indonesian Journal of Mathematics and Natural Sciences*, *46*(2), 61–67. https://doi.org/10.15294/ijmns.v46i2.47250

DOI: https://doi.org/10.31004/riggs.v4i2.1118