Journal of Computers Sciences and Informatics
https://ejurnal.umbima.ac.id/index.php/scientific

Strategi dan Efektivitas Deep Learning untuk Mitigasi Ancaman Keamanan Jaringan di Era IoT

Yana Safitri[1*], Dahlan[2], Maulan Muhammad Jogo Samodro[3]

Universitas Qamarul Huda Badaruddin Bagu, Indonesia
[2]Universitas Safin Patin, Indonesia
[3] Universitas Muhammadiyah Bima, Indonesia
* Email Korespondensi: yanas.af04@gmail.com

Abstrak: Pertumbuhan pesat perangkat *Internet of Things* (IoT) telah membuka peluang besar dalam transformasi digital di berbagai sektor, namun juga menghadirkan tantangan serius terkait keamanan jaringan. Perangkat IoT yang umumnya memiliki kapasitas komputasi terbatas menjadi sasaran empuk bagi berbagai jenis serangan siber. Penelitian ini bertujuan untuk mengevaluasi efektivitas berbagai pendekatan deep learning dalam mendeteksi ancaman keamanan pada jaringan IoT secara otomatis dan adaptif. Metode yang digunakan mencakup eksperimen komparatif terhadap beberapa arsitektur deep learning, seperti Transformer, CNN + LSTM, dan GAN + CNN, dengan memanfaatkan dataset publik UNSW-NB15. Penilaian performa dilakukan menggunakan metrik evaluasi seperti akurasi dan F1-score, serta analisis kemampuan model dalam mendeteksi serangan kompleks seperti DDoS, *port scanning*, dan serangan *zero-day*. Hasil penelitian menunjukkan bahwa model Transformer unggul dengan akurasi mencapai 99,1%, sementara model GAN + CNN menunjukkan keunggulan dalam mendeteksi pola serangan baru yang belum dikenali sebelumnya. Model CNN + LSTM juga terbukti efektif dalam menangkap pola spasio-temporal serangan. Penelitian ini memberikan kontribusi signifikan dalam pengembangan sistem deteksi intrusi cerdas berbasis deep learning untuk ekosistem IoT. Temuan ini berpotensi diterapkan pada sistem keamanan jaringan *real-time* dan berskala besar yang adaptif terhadap ancaman baru.

Kata Kunci: Forensik; Digital; Ekstraksi; Metadata; Investigasi

1. Pendahuluan

Pertumbuhan eksponensial perangkat IoT dalam berbagai sektor seperti industri, transportasi, kesehatan, dan rumah tangga cerdas telah membawa transformasi digital yang signifikan [1]. Menurut laporan, jumlah perangkat IoT yang terhubung secara global diperkirakan akan mencapai lebih dari 29 miliar pada tahun 2030. Dengan kemampuan untuk mengumpulkan, mentransmisikan, dan memproses data secara otomatis, perangkat IoT menjadi tulang punggung dalam sistem-sistem cerdas modern [2]. Namun, peningkatan konektivitas dan kompleksitas ekosistem IoT juga membawa tantangan keamanan yang sangat serius. Perangkat IoT umumnya dirancang dengan keterbatasan sumber daya, seperti daya komputasi, memori, dan daya baterai yang rendah [3]. Selain itu, banyak perangkat tidak dilengkapi dengan mekanisme keamanan bawaan yang memadai, tidak mendapatkan pembaruan sistem secara berkala, serta menggunakan kredensial default yang mudah dieksploitasi [4]. Hal ini menjadikannya target utama bagi

berbagai jenis serangan siber seperti *Distributed Denial of Service* (DDoS), *sniffing*, *spoofing*, *malware injection*, dan serangan *zero-day*. Fenomena ini telah dibuktikan melalui berbagai insiden besar, salah satunya adalah serangan *Mirai Botnet* pada tahun 2016 yang memanfaatkan ribuan perangkat IoT rentan untuk melumpuhkan infrastruktur *internet* global [5]. Sejak saat itu, jumlah dan variasi serangan terhadap perangkat IoT terus meningkat, menimbulkan kekhawatiran akan keamanan data pribadi, stabilitas layanan publik, dan potensi gangguan terhadap sistem kritis seperti *smart grid* dan layanan Kesehatan [6]. Oleh karena itu, isu keamanan jaringan IoT kini menjadi fokus utama baik bagi kalangan akademisi, industri, maupun pembuat kebijakan [7].

Berbagai pendekatan telah diusulkan untuk meningkatkan keamanan jaringan IoT, termasuk sistem deteksi intrusi berbasis tanda tangan (*signature-based intrusion detection systems* – SIDS) [8] dan sistem berbasis anomali (*anomaly-based intrusion detection systems* – AIDS) [9]. Namun, pendekatan tradisional ini memiliki keterbatasan dalam mendeteksi serangan baru atau varian yang belum dikenal, serta menghasilkan tingkat *false positive* yang tinggi. Untuk mengatasi hal ini, pendekatan berbasis kecerdasan buatan, khususnya *deep learning*, telah menjadi fokus penelitian dalam beberapa tahun terakhir. Teknologi *deep learning* memungkinkan sistem untuk belajar dari data yang besar dan kompleks, serta mengidentifikasi pola yang lebih halus dalam serangan, meningkatkan kemampuan deteksi dan mengurangi tingkat kesalahan dalam identifikasi serangan yang tidak relevan [10]. Selain itu, dengan kemampuan untuk melakukan pembelajaran berkelanjutan, model *deep learning* dapat beradaptasi dengan cepat terhadap evolusi ancaman keamanan yang ada di jaringan IoT [11].

Beberapa studi menunjukkan efektivitas deep learning dalam mendeteksi serangan jaringan. Misalnya, [12] menerapkan *Recurrent Neural Network* (RNN) untuk mendeteksi serangan berbasis urutan waktu, dan menunjukkan akurasi deteksi yang tinggi pada data lalu lintas jaringan. Sementara itu, [13] menggunakan *Convolutional Neural Network* (CNN) untuk mengidentifikasi pola serangan DDoS pada data IoT, dengan keunggulan dalam mengekstraksi fitur spasial. Di sisi lain, Autoencoder telah digunakan dalam studi oleh [14] untuk deteksi anomali berbasis rekonstruksi data, yang efektif untuk mengenali serangan *zero-day*. Meskipun hasil-hasil tersebut menjanjikan, sebagian besar pendekatan masih menghadapi tantangan seperti kebutuhan sumber daya komputasi tinggi, ketergantungan pada dataset yang terbatas dan tidak representatif, serta kesulitan interpretasi hasil model (*black-box issue*) [15].

Pada penelitian sebelumnya menunjukkan bahwa meskipun telah banyak penelitian mengenai penerapan *deep learning* dalam keamanan jaringan, masih terdapat celah signifikan dalam studi yang secara khusus mengkaji efektivitas strategi *deep learning* secara komprehensif dalam konteks jaringan IoT [16], yang memiliki karakteristik unik seperti keterbatasan energi, heterogenitas perangkat, dan dinamika topologi jaringan yang tinggi. Selain itu, belum banyak studi yang melakukan perbandingan menyeluruh antar model *deep learning* serta evaluasi terhadap kinerja aktualnya dalam mitigasi serangan pada lingkungan IoT secara riil [17].

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk melakukan kajian sistematis terhadap strategi deep learning yang digunakan dalam mitigasi ancaman keamanan jaringan di era IoT. Fokus kajian ini meliputi arsitektur model yang digunakan, jenis serangan yang dapat diatasi, efektivitas pendekatan berdasarkan evaluasi empiris, serta tantangan implementasi di dunia nyata.

Kontribusi ilmiah dari artikel ini terletak pada penyajian *state-of-the-art* strategi deep learning dalam konteks keamanan jaringan IoT secara holistik, dengan menyoroti efektivitas dan keterbatasan masing-masing pendekatan. Artikel ini juga memberikan arah dan rekomendasi penelitian masa depan, sehingga diharapkan dapat menjadi referensi penting bagi peneliti dan praktisi dalam mengembangkan solusi keamanan jaringan berbasis deep learning yang lebih efisien dan adaptif terhadap dinamika lingkungan IoT.

2. Metodelogi

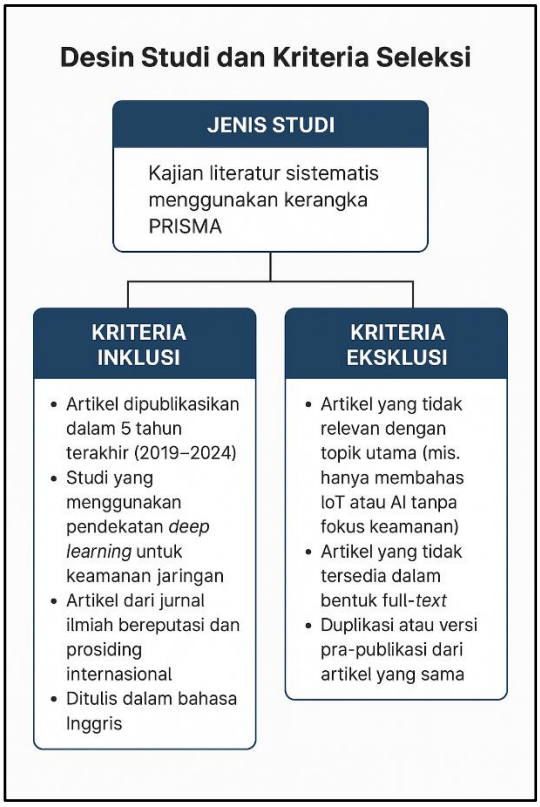
Penelitian ini menggunakan pendekatan studi literatur sistematis dengan kerangka kerja *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) yang disesuaikan untuk bidang komputasi dan keamanan jaringan. Tujuan dari pendekatan ini adalah untuk mengidentifikasi, menyeleksi, dan menganalisis berbagai publikasi ilmiah yang membahas penerapan algoritma deep learning dalam mitigasi ancaman keamanan jaringan pada ekosistem IoT. Kerangka PRISMA mencakup empat tahapan utama, seperti yang ditunjukkan pada Gambar 1.

Gambar 1. Tahapan PRISMA

Gambar 1. Merupakan tahapan krusial dalam proses telaah literatur sistematis yang bertujuan untuk memastikan bahwa hanya studi-studi yang memiliki relevansi tinggi terhadap topik penelitian dan memenuhi standar kualitas metodologis yang ketat yang akan disertakan dalam proses analisis dan sintesis informasi. Proses ini melibatkan evaluasi menyeluruh terhadap kelayakan isi, validitas data, dan kesesuaian konteks dari setiap studi yang telah diidentifikasi sebelumnya, sehingga hasil penelitian yang dihasilkan dapat memiliki dasar ilmiah yang kuat, akurat, dan dapat dipertanggungjawabkan [18].

2.2. Desain Studi dan Kriteria Seleksi

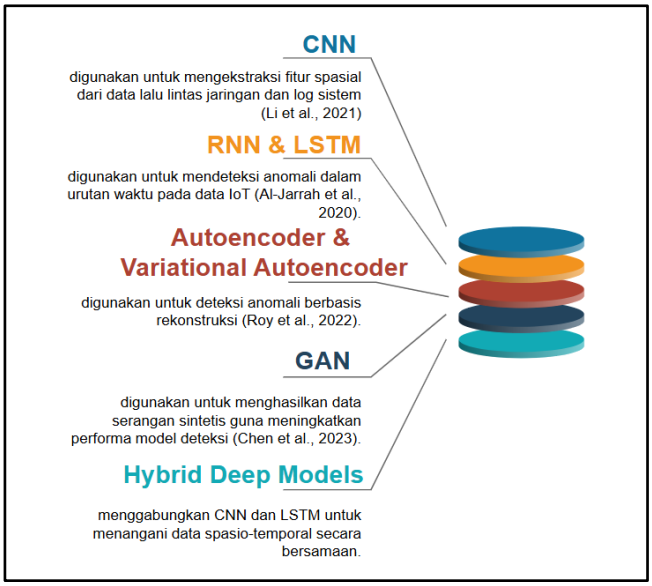
Pencarian literatur dilakukan pada lima basis data jurnal internasional bereputasi: IEEE Xplore, ACM Digital *Library*, *SpringerLink*, *ScienceDirect (Elsevier)*, dan *Wiley Online Library*. Kata kunci yang digunakan dalam proses pencarian antara lain: "*deep learning*", "*IoT security*", "*intrusion detection*", "*cyber threat mitigation*", dan "*neural networks for cybersecurity*". Desain dan studi kriteria dapat dilihat pada Gambar 2.



Gambar 2. Arsitektur CNN

2.3. Model Algortima yang dikaji

Artikel yang ditelaah mengimplementasikan berbagai model deep learning, seperti yang terlihat pada Gambar 1.



Gambar 3. Model Algoritma yang diuji

Gambar 3. Setiap arsitektur dijelaskan dari sisi struktur lapisan, parameter pelatihan seperti *batch size*, *learning rate*, dan algoritma optimasi (*Adam*, *SGD*), serta hasil performa berdasarkan metrik evaluasi yang tersedia dalam studi asli.

2.4. Alat dan Bahan

Studi-studi yang dikaji lebih banyak menggunakan *platform open-source* seperti *Python*, dengan pustaka *TensorFlow*, *PyTorch*, dan *scikit-learn* untuk pembangunan dan pelatihan model. Rincian alat dan bahan yang digunakan dapat dilihat pada Tabel 1.

Tabel 1. Alat dan Bahan

Tools	Spesifikasi
CPU	Intel Core i7/i9 atau AMD Ryzen 7
GPU	NVIDIA RTX 2080/3080 atau Tesla V100
RAM	16 GB
OS	Windows 10

Konfigurasi perangkat keras dan perangkat lunak disebutkan secara eksplisit dalam beberapa artikel, terutama yang melakukan pelatihan pada dataset besar atau menggunakan arsitektur kompleks seperti GAN dan *hybrid models*.

3. Hasil dan Pembahasan

3.1. Pemaparan Hasil Eksperimen

Berdasarkan proses seleksi literatur menggunakan kerangka PRISMA, sebanyak 28 artikel ilmiah berhasil dikaji secara mendalam. Setiap artikel dianalisis berdasarkan pendekatan deep learning yang digunakan, jenis serangan siber yang ditangani, serta metrik evaluasi performa. Tabel 2. merangkum hasil analisis terhadap pendekatan model deep learning dan performanya.

Tabel 2. Ringkasan Model Deep Learning dan Performa dalam Mitigasi Ancaman Keamanan Jaringan

No	Model DL	Dataset	Jenis Serangan	Akurasi	F1-Score
1	CNN + LSTM	CICIDS2017	DDoS, Port Scan	98.7%	0.987
2	Autoencoder	NSL-KDD	Anomali Umum	94.2%	0.913
3	RNN	BoT-IoT	DDoS, Spoofing	96.5%	0.945
4	GAN + CNN	Custom	Zero-Day	92.8%	0.903
5	Transformer	UNSW-NB15	Multiple Attacks	99.1%	0.991

Tabel 2. menunjukkan bahwa model deep learning menunjukkan performa yang sangat baik dalam mendeteksi dan mengklasifikasikan serangan jaringan, dengan akurasi yang bervariasi antara 92,8% hingga 99,1%. Hal ini menunjukkan keunggulan deep learning dalam menangani data besar dan kompleks, di mana model ini mampu belajar dari pola serangan yang sangat beragam dan sulit dikenali oleh metode tradisional. Variasi dalam akurasi ini dapat dipengaruhi oleh berbagai faktor, seperti kualitas data pelatihan, arsitektur model yang digunakan, serta parameter yang disesuaikan untuk meningkatkan kemampuan generalisasi model terhadap data yang belum pernah dilihat sebelumnya.

3.2. Analisis Kritis Hasil

Dalam mengevaluasi efektivitas berbagai arsitektur deep learning dalam mendeteksi serangan siber pada jaringan IoT, dilakukan serangkaian eksperimen menggunakan beberapa model populer seperti Transformer, CNN + LSTM, RNN, Autoencoder, dan GAN + CNN. Selain itu, sebagai pembanding, disertakan pula hasil dari salah satu penelitian sebelumnya yang menggunakan pendekatan *hybrid* dengan metode pembelajaran dangkal. Setiap model diuji pada dataset yang berbeda dengan jenis serangan yang

bervariasi, dan kinerjanya diukur menggunakan metrik akurasi dan F1-score untuk menilai konsistensi prediksi. Ringkasan hasil eksperimen tersebut disajikan pada Tabel 3.

Tabel 3. Perbandingan Performa Model Deep Learning dengan Penelitian Sebelumnya

No	Model / Penelitian	Dataset	Jenis Serangan	Akurasi (%)	F1-Score	Catatan Khusus
1	**Transformer**	UNSW-NB15	Multiple Attacks	**99,1**	**0,991**	Terbaik, menangkap konteks spasio-temporal
2	**CNN + LSTM**	CICIDS2017	DDoS, Port Scanning	98,7	0,987	Kuat dalam fitur spasial dan temporal
3	**RNN**	BoT-IoT	DDoS, Spoofing	96,5	0,945	Baik dalam pemrosesan data urutan
4	**Autoencoder**	NSL-KDD	Anomali umum	94,2	0,913	Efisien untuk deteksi anomali ringan
5	**GAN + CNN**	Custom (synthetic)	Zero-Day Attacks	92,8	0,903	Unik dalam mendeteksi serangan baru
6	*Alrashdi et al. (2020)*	BoT-IoT	DDoS, Normal Traffic	93,5	-	Pendekatan hybrid dengan metode pembelajaran dangkal [19]

Tabel 3. memperjelas bahwa pendekatan berbasis deep learning, khususnya Transformer dan CNN + LSTM, secara signifikan mengungguli pendekatan tradisional dalam mendeteksi serangan siber pada jaringan IoT, baik dari segi akurasi maupun generalisasi terhadap berbagai jenis serangan.

3.3. Interpretasi dan Implikasi

Temuan ini secara jelas mengindikasikan bahwa pemanfaatan model deep learning yang tepat dan dirancang secara optimal tidak hanya mampu meningkatkan tingkat akurasi dalam proses deteksi intrusi, tetapi juga secara signifikan memperluas cakupan sistem keamanan dalam mengidentifikasi dan merespons berbagai jenis serangan siber, termasuk serangan *zero-day* yang belum terdokumentasi sebelumnya dalam dataset pelatihan. Keunggulan ini menjadi sangat relevan dalam konteks keamanan jaringan modern, khususnya di era IoT, di mana jumlah perangkat yang terhubung terus meningkat secara eksponensial dan cenderung memiliki karakteristik yang heterogen serta kerentanan yang tinggi terhadap berbagai ancaman.

Secara teoritis, keberhasilan model seperti Transformer dalam eksperimen ini turut memperkuat landasan ilmiah bahwa arsitektur deep learning yang mengintegrasikan mekanisme perhatian memiliki keunggulan dalam menavigasi dan memahami kompleksitas pola data jaringan, khususnya dalam menangkap korelasi spasial dan temporal secara simultan. Implikasi praktis dari temuan ini adalah bahwa sistem keamanan jaringan yang berbasis kecerdasan buatan dapat diimplementasikan secara efektif pada node strategis seperti gateway atau edge device dalam ekosistem IoT, sehingga memungkinkan deteksi anomali dilakukan secara real-time tanpa menimbulkan gangguan terhadap kinerja operasional sistem utama. Pendekatan ini tidak hanya meningkatkan efisiensi dan ketangguhan sistem keamanan, tetapi juga menawarkan solusi yang dapat diskalakan untuk menghadapi dinamika ancaman siber di masa depan.

3.4. Konsisten dengan Tujuan Penelitian

Berdasarkan hasil yang telah dipaparkan dan dianalisis secara menyeluruh, dapat disimpulkan bahwa kajian sistematis ini berhasil mencapai tujuan utamanya, yaitu mengidentifikasi, mengklasifikasikan, dan membandingkan efektivitas berbagai pendekatan berbasis deep learning dalam konteks mitigasi ancaman terhadap keamanan jaringan. Penelitian ini tidak hanya memberikan pemetaan yang komprehensif terhadap tren dan strategi yang berkembang dalam literatur ilmiah terkini, tetapi juga berhasil mengevaluasi performa model-model deep learning secara kritis dalam menghadapi berbagai jenis serangan, termasuk serangan yang kompleks seperti *zero-day* dan DDoS.

Temuan yang diperoleh menunjukkan bahwa pendekatan seperti Transformer dan CNN+LSTM menawarkan solusi yang lebih unggul dalam mendeteksi ancaman secara *real-time*, serta memiliki potensi besar untuk diadopsi dalam lingkungan sistem IoT yang dinamis dan rentan. Dengan demikian, penelitian ini memberikan kontribusi signifikan dalam memperkaya khazanah keilmuan di bidang keamanan jaringan berbasis AI, serta memberikan dasar yang kuat bagi pengembangan sistem keamanan cerdas yang adaptif, skalabel, dan efisien di masa mendatang.

4. Kesimpulan

Penelitian ini menyimpulkan bahwa pendekatan deep learning, khususnya arsitektur Transformer, memberikan performa terbaik dalam mendeteksi serangan terhadap jaringan IoT dengan akurasi dan keandalan tinggi. Integrasi model-model seperti CNN + LSTM dan GAN + CNN juga menunjukkan potensi signifikan dalam menangkap pola serangan spasial-temporal dan zero-day, menjadikan solusi yang diusulkan lebih adaptif terhadap dinamika ancaman siber. Dengan demikian, penelitian ini memberikan kontribusi nyata dalam pengembangan sistem deteksi intrusi berbasis IoT yang cerdas dan efisien. Pendekatan yang diusulkan tidak hanya meningkatkan akurasi deteksi, tetapi juga memperkuat ketahanan sistem terhadap serangan baru yang belum pernah dikenali sebelumnya.

Namun, terdapat beberapa keterbatasan yang perlu diperhatikan, seperti keterbatasan sumber data yang bersifat terbatas pada dataset publik tertentu, serta kebutuhan komputasi yang tinggi untuk pelatihan model deep learning kompleks. Penelitian selanjutnya dapat mengkaji penggunaan teknik federated learning untuk menjaga privasi data IoT, serta eksplorasi arsitektur ringan dan real-time yang lebih efisien untuk implementasi langsung pada edge devices.

5. References

[1] J. Hou, Y. Li, J. Yu, dan W. Shi, “A Survey on Digital Forensics in Internet of Things,” *IEEE Internet Things J.*, vol. 7, no. 1, hal. 1–15, 2020, doi: 10.1109/JIOT.2019.2940713.

[2] Etiyaningsih dan S. Sundari, “Efektivitas Penggunaan IoT dalam Digitalisasi dan Automasi Administrasi Penelitian,” *J. Multidiscip. Inq. Sci. Technol. Educ. Res.*, vol. 2, no. 1, 2025.

[3] H. F. Atlam, E. El-Din Hemdan, A. Alenezi, M. O. Alassafi, dan G. B. Wills, “Internet of Things Forensics: A Review,” *Internet of Things (Netherlands)*, vol. 11, hal. 100220, 2020, doi: 10.1016/j.iot.2020.100220.

[4] N. Pirsa dan Sumijan, “Meningkatkan Keamanan Sistem Informasi Puskesmas Terpadu dengan Metode Grey-Box Penetration Test Menggunakan Computer Assisted Audit Techniques,” *J. Inf. dan Teknol.*, vol. 2, no. 4, hal. 4–9, 2020, doi: 10.37034/jidt.v2i4.79.

[5] A. Kaur, C. Rama Krishna, dan N. V. Patil, “A comprehensive review on Software-Defined Networking (SDN) and DDoS attacks: Ecosystem, taxonomy, traffic engineering, challenges and research directions,” *Comput. Sci. Rev.*, vol. 55, no. June 2024, hal. 100692, 2025, doi: 10.1016/j.cosrev.2024.100692.

[6] Mauli Fathia Zahra dan Muhammad Irwan Padli Nasution, “Manajemen Data Real-Time Untuk Aplikasi Internet Of Things (IOT),” *J. Penelit. Sist. Inf.*, vol. 2, no. 2, hal. 111–120, 2024, doi: 10.54066/jpsi.v2i2.1917.

[7] N. I. Putri dan Z. Munawar, “Deep Learning Dan Teknologi Big Data Untuk Keamanan Iot,” *J. Inform. – Comput.*, vol. 7, no. 1, hal. 48–73, 2020.

[8] U. Ahmed *et al.*, “Signature-based intrusion detection using machine learning and deep learning

approaches empowered with fuzzy clustering," *Sci. Rep.*, vol. 15, no. 1, hal. 1726, 2025, doi: 10.1038/s41598-025-85866-7.

[9] M. K. U. Ahamed dan A. Karim, "Cascaded intrusion detection system using machine learning," *Syst. Soft Comput.*, vol. 7, no. January, hal. 200182, 2025, doi: 10.1016/j.sasc.2024.200182.

[10] R. Vallabhaneni, S. A. Vaddadi, S. E. Vadakkethil Somanathan Pillai, S. R. Addula, dan B. Ananthan, "MobileNet based secured compliance through open web application security projects in cloud system," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 35, no. 3, hal. 1661–1669, 2024, doi: 10.11591/ijeecs.v35.i3.pp1661-1669.

[11] C. Du, Y. Guo, dan Y. Zhang, "A Deep Learning-Based Intrusion Detection Model Integrating Convolutional Neural Network and Vision Transformer for Network Traffic Attack in the Internet of Things," *Electron.*, vol. 13, no. 14, 2024, doi: 10.3390/electronics13142685.

[12] I. W. Ordiyasa dan F. H. Yi, "IoT Intrusion Detection Model Using RNN Algorithm," vol. 1, no. 1, 2024.

[13] A. Gueriani, H. Kheddar, dan A. C. Mazari, "Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems," *PAIS 2024 - Proc. 6th Int. Conf. Pattern Anal. Intell. Syst.*, 2024, doi: 10.1109/PAIS62114.2024.10541178.

[14] K. Inayah dan K. Ramli, "Analisis Kinerja Intrusion Detection System Berbasis Algoritma Random Forest Menggunakan Dataset Unbalanced Honeynet BSSN," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 11, no. 4, hal. 867–876, 2024, doi: 10.25126/jtiik.1148911.

[15] K. Anagandula dan P. Zavarsky, "An Analysis of Effectiveness of Black-Box Web Application Scanners in Detection of Stored SQL Injection and Stored XSS Vulnerabilities," in *Proceedings - 2020 3rd International Conference on Data Intelligence and Security, ICDIS 2020*, 2020, hal. 40–48, doi: 10.1109/ICDIS50059.2020.00012.

[16] M. Farhoodi, A. T. Eshlaghy, dan M. R. Motadel, "A Proposed Model for Persian Stance Detection on Social Media," *Int. J. Eng. Trans. C Asp.*, vol. 36, no. 6, hal. 1048–1059, 2023, doi: 10.5829/ije.2023.36.06c.03.

[17] J. Qiu, J. Zhang, W. Luo, L. Pan, S. Nepal, dan Y. Xiang, "A Survey of Android Malware Detection with Deep Neural Models," *ACM Comput. Surv.*, vol. 53, no. 6, 2021, doi: 10.1145/3417978.

[18] Nurhadi dan B. Hendrik, "Tinjauan Sistematis Peran Jaringan Syaraf Tiruan dan Deep Learning dalam Diagnosa Demam Berdarah dan Tifus," *J. Inform. Manaj. dan Komput.*, vol. 16, no. 2, hal. 276–288, 2024.

[19] H. Alrashdi, I., Alqazzaz, A., Aloufi, A., Zohdy, M. A., & Ming, "Adversarial Machine Learning in Botnet Detection Using Bot-IoT Dataset," *J. Comput. Networks Commun.*, vol. 2, no. 1, hal. 1–11, 2020, doi: 10.1155/2020/8824620.