KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik (JMIA)
Vol.3, No.2 April 2026
e-ISSN: 3032-7377, p-ISSN : 3032-7385, Hal 621-630
DOI : https://doi.org/10.61722/jmia.v3i2.9425

Optimasi Sistem Deteksi Intrusi Berbasis Deep Neural Network dengan Seleksi Fitur Adaptif pada Jaringan Komputer Modern

Hafidzun Alim[1*]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Industri dan Informatika, Universitas Muhammadiyah Prof Dr. Hamka (UHAMKA)
*Penulis Korespondensi: alimarsena@gmail.com

Abstract. *The increasing complexity and sophistication of cyber threats in modern computer networks has driven the need for more intelligent and adaptive Intrusion Detection Systems (IDS). This study proposes an optimization of a Deep Neural Network (DNN)-based Intrusion Detection System combined with an Adaptive Feature Selection mechanism to improve detection accuracy while reducing computational complexity. The research employs the CICIDS-2017 and NSL-KDD benchmark datasets, applying a hybrid feature selection approach that integrates filter methods (mutual information and chi-square) with wrapper methods (recursive feature elimination) to select the most discriminative feature subsets. The proposed DNN architecture consists of multiple hidden layers with batch normalization and dropout regularization to prevent overfitting. Experimental results demonstrate that the proposed system achieves a detection accuracy of 99.41%, a precision of 98.87%, recall of 99.12%, and an F1-score of 98.99% on the CICIDS-2017 dataset, outperforming existing methods. The adaptive feature selection method effectively reduces the feature dimension by 62.3%, resulting in a 45.7% reduction in training time without sacrificing detection performance. The system demonstrates robust performance against zero-day attacks and encrypted traffic. These findings confirm that the integration of deep learning with adaptive feature selection constitutes an effective strategy for building next-generation intrusion detection systems in modern network environments*
Keywords: *Adaptive Feature Selection; Deep Neural Network; Intrusion Detection System; Machine Learning; Network Security.*

Abstrak. Meningkatnya kompleksitas dan kecanggihan ancaman siber pada jaringan komputer modern mendorong kebutuhan akan Sistem Deteksi Intrusi (IDS) yang lebih cerdas dan adaptif. Penelitian ini mengusulkan optimasi Sistem Deteksi Intrusi berbasis Deep Neural Network (DNN) yang dikombinasikan dengan mekanisme Seleksi Fitur Adaptif untuk meningkatkan akurasi deteksi sekaligus mengurangi kompleksitas komputasi. Penelitian menggunakan dataset benchmark CICIDS-2017 dan NSL-KDD, menerapkan pendekatan seleksi fitur hibrida yang mengintegrasikan metode filter (mutual information dan chi-square) dengan metode wrapper (recursive feature elimination) untuk memilih subset fitur paling diskriminatif. Arsitektur DNN yang diusulkan terdiri dari beberapa hidden layer dengan batch normalization dan dropout regularization untuk mencegah overfitting. Hasil eksperimen menunjukkan bahwa sistem yang diusulkan mencapai akurasi deteksi 99,41%, presisi 98,87%, recall 99,12%, dan F1-score 98,99% pada dataset CICIDS-2017, melampaui metode yang ada. Metode seleksi fitur adaptif secara efektif mengurangi dimensi fitur sebesar 62,3%, menghasilkan pengurangan waktu pelatihan sebesar 45,7% tanpa mengorbankan kinerja deteksi. Sistem menunjukkan kinerja yang tangguh terhadap serangan zero-day dan lalu lintas terenkripsi. Temuan ini mengonfirmasi bahwa integrasi deep learning dengan seleksi fitur adaptif merupakan strategi efektif untuk membangun sistem deteksi intrusi generasi berikutnya pada lingkungan jaringan komputer modern.
Kata kunci: Deep Neural Network; Jaringan Komputer; Keamanan Jaringan; Seleksi Fitur Adaptif; Sistem Deteksi Intrusi.

LATAR BELAKANG

Perkembangan teknologi jaringan komputer yang pesat dalam dekade terakhir telah menghadirkan berbagai tantangan keamanan yang semakin kompleks. Serangan siber terus berkembang dalam hal kecanggihan, volume, dan variasi, sehingga sistem

Naskah Masuk: 05 Maret 2026; Revisi: 10 Maret 2026; Diterima: 04 April 2026; Terbit: 04 April 2026

keamanan tradisional semakin tidak mampu menghadapinya secara efektif *(Ferrag et al., 2022)*. Sistem Deteksi Intrusi (IDS) merupakan komponen kritis dalam infrastruktur keamanan jaringan yang berfungsi untuk mengidentifikasi aktivitas anomali dan potensi serangan *(Liu et al., 2023)*. Namun, IDS berbasis aturan (rule-based) yang konvensional memiliki keterbatasan signifikan dalam mendeteksi serangan baru yang belum pernah teridentifikasi sebelumnya atau yang dikenal sebagai zero-day attacks *(Thakkar & Lohiya, 2021)*.

Pendekatan machine learning, khususnya deep learning, telah terbukti menjanjikan sebagai solusi untuk mengatasi keterbatasan IDS tradisional *(Lansky et al., 2021)*. Deep Neural Network (DNN) mampu mempelajari representasi fitur yang kompleks dan hierarkis dari data lalu lintas jaringan, sehingga dapat mendeteksi pola serangan yang rumit tanpa bergantung pada aturan yang telah didefinisikan secara manual *(Aldweesh et al., 2020)*. Berbagai arsitektur deep learning seperti Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), dan Long Short-Term Memory (LSTM) telah diaplikasikan pada domain deteksi intrusi dengan hasil yang beragam *(Ullah & Mahmoud, 2021)*.

Meskipun demikian, penerapan DNN pada IDS masih menghadapi beberapa tantangan utama. Pertama, data lalu lintas jaringan memiliki dimensionalitas yang sangat tinggi, yang dapat menyebabkan fenomena 'curse of dimensionality' sehingga menurunkan performa model *(Sarhan et al., 2021)*. Kedua, keberadaan fitur-fitur yang tidak relevan atau redundan dapat mengganggu proses pembelajaran dan meningkatkan waktu komputasi secara signifikan *(Kasongo & Sun, 2022)*. Ketiga, ketidakseimbangan kelas (class imbalance) pada dataset jaringan yang umum, di mana trafik normal jauh lebih dominan dibandingkan trafik serangan, dapat menyebabkan bias pada model yang dilatih *(Roshan & Zafar, 2021)*.

Seleksi fitur merupakan langkah pre-processing krusial yang bertujuan untuk memilih subset fitur yang paling informatif dan relevan dari data asli *(Shafiq et al., 2022)*. Teknik seleksi fitur dapat secara signifikan meningkatkan akurasi model, mengurangi overfitting, mempercepat waktu pelatihan, serta meningkatkan interpretabilitas model *(Gao et al., 2022)*. Pendekatan seleksi fitur adaptif yang mampu menyesuaikan diri dengan karakteristik data yang berubah secara dinamis menjadi kebutuhan mendesak dalam sistem IDS modern *(Zhang et al., 2023)*.

Berdasarkan kajian terhadap penelitian terdahulu, terdapat kesenjangan (gap) yang signifikan dalam pengembangan IDS berbasis DNN. Mayoritas penelitian yang ada menggunakan pendekatan seleksi fitur statis yang tidak mampu beradaptasi dengan perubahan pola serangan yang dinamis *(Xu et al., 2021)*. Selain itu, banyak penelitian hanya dievaluasi pada satu dataset benchmark sehingga generalisasi modelnya masih dipertanyakan *(Basnet et al., 2021)*. Penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan mengusulkan sistem IDS yang mengintegrasikan DNN dengan mekanisme Seleksi Fitur Adaptif (Adaptive Feature Selection/AFS) yang mampu bekerja secara optimal pada berbagai kondisi jaringan dan pola serangan yang beragam.

KAJIAN TEORITIS

A. Sistem Deteksi Intrusi (IDS)

Sistem Deteksi Intrusi (IDS) adalah sistem yang memantau lalu lintas jaringan atau aktivitas sistem untuk mengidentifikasi tanda-tanda serangan atau penyalahgunaan (Liao et al., 2021). Secara umum, IDS diklasifikasikan menjadi dua kategori utama: Network-based IDS (NIDS) yang memantau paket jaringan, dan Host-based IDS (HIDS) yang memantau aktivitas pada sistem tertentu (Khraisat et al., 2019). Dari sisi metodologi deteksi, IDS dibedakan menjadi signature-based detection yang mencocokkan pola serangan yang sudah diketahui, dan anomaly-based detection yang mengidentifikasi deviasi dari perilaku normal (Thakkar & Lohiya, 2021). Pendekatan anomaly-based memiliki keunggulan dalam mendeteksi serangan baru, namun rentan terhadap tingkat false positive yang tinggi (Ferrag et al., 2022).

B. Deep Neural Network untuk Deteksi Intrusi

Deep Neural Network (DNN) adalah jaringan saraf tiruan dengan banyak lapisan tersembunyi yang mampu mempelajari representasi fitur hierarkis dari data mentah (Goodfellow et al., 2016). Dalam konteks deteksi intrusi, DNN telah menunjukkan kemampuan superior dalam mengekstrak pola kompleks dari data lalu lintas jaringan (Ullah & Mahmoud, 2021). Penelitian oleh Lansky et al. (2021) menunjukkan bahwa DNN dengan arsitektur multi-layer mampu mencapai akurasi deteksi yang jauh lebih tinggi dibandingkan algoritma machine learning klasik seperti SVM dan Random Forest pada dataset NSL-KDD. Arsitektur DNN yang optimal untuk IDS umumnya mencakup lapisan input normalisasi, beberapa hidden layer dengan aktivasi ReLU, batch normalization untuk menstabilkan proses pelatihan, dropout untuk regularisasi, dan lapisan output softmax untuk klasifikasi multi-kelas (Kasongo & Sun, 2022).

Variasi arsitektur deep learning lainnya juga telah dieksplorasi secara intensif. CNN telah diterapkan untuk mengekstrak fitur lokal dari representasi data jaringan berbasis gambar (Gao et al., 2022). LSTM dan Gated Recurrent Unit (GRU) memanfaatkan sifat sekuensial dari lalu lintas jaringan untuk mendeteksi serangan yang tersebar dalam jangka waktu tertentu (Zhang et al., 2023). Model hybrid yang menggabungkan CNN dan LSTM (CNN-LSTM) telah menunjukkan hasil yang menjanjikan dalam menangkap fitur spasial dan temporal secara simultan (Xu et al., 2021). Mekanisme attention juga telah

diintegrasikan ke dalam DNN untuk meningkatkan fokus pada fitur-fitur yang paling relevan (Shafiq et al., 2022).

C. Seleksi Fitur Adaptif

Seleksi fitur adalah proses memilih subset fitur yang paling relevan dan informatif dari dataset untuk digunakan dalam proses pelatihan model (Sarhan et al., 2021). Terdapat tiga kategori utama metode seleksi fitur: (1) Filter methods yang mengevaluasi relevansi fitur berdasarkan ukuran statistik seperti information gain, chi-square, atau korelasi Pearson, secara independen dari algoritma pembelajaran; (2) Wrapper methods yang menggunakan performa model machine learning sebagai kriteria evaluasi subset fitur, seperti Recursive Feature Elimination (RFE); dan (3) Embedded methods yang mengintegrasikan seleksi fitur ke dalam proses pelatihan model, seperti L1 regularization (LASSO) (Roshan & Zafar, 2021).

Pendekatan seleksi fitur adaptif mengacu pada kemampuan sistem untuk secara dinamis menyesuaikan subset fitur yang dipilih berdasarkan perubahan distribusi data atau lingkungan operasional (Liu et al., 2023). Metode hibrida yang mengkombinasikan filter dan wrapper methods telah terbukti efektif dalam menyeimbangkan efisiensi komputasi dan akurasi seleksi fitur (Basnet et al., 2021). Pada konteks IDS, pendekatan adaptif sangat penting karena pola serangan terus berkembang, sehingga fitur yang relevan pada suatu waktu mungkin tidak lagi optimal pada periode berikutnya (Kasongo & Sun, 2022).

D. Penelitian Terdahulu

Sejumlah penelitian terdahulu telah berupaya mengoptimalkan IDS berbasis deep learning. Ferrag et al. (2022) melakukan tinjauan sistematis terhadap metode IDS berbasis deep learning dan menemukan bahwa CNN-LSTM hybrid memberikan performa terbaik pada dataset CICIDS-2017 dengan akurasi 98,73%. Zhang et al. (2023) mengusulkan IDS berbasis Graph Neural Network (GNN) yang mampu memodelkan hubungan antar entitas jaringan, mencapai F1-score sebesar 97,89% pada dataset CIC-DDoS2019. Shafiq et al. (2022) mengintegrasikan mekanisme attention berbasis transformer dengan seleksi fitur berbasis mutual information, menghasilkan peningkatan akurasi sebesar 2,3% dibandingkan metode baseline pada NSL-KDD. Gao et al. (2022) mengembangkan metode seleksi fitur berbasis AutoEncoder yang mampu menemukan representasi fitur optimal secara unsupervised, mengurangi dimensi fitur sebesar 58% dengan penurunan

akurasi minimal. Penelitian-penelitian tersebut menunjukkan tren yang konsisten menuju integrasi deep learning dengan teknik seleksi fitur yang lebih canggih, namun pendekatan adaptif yang komprehensif masih jarang dieksplorasi.

METODE PENELITIAN

Penelitian ini menggunakan dua dataset benchmark yang umum digunakan dalam penelitian IDS. Dataset pertama adalah CICIDS-2017 yang dikembangkan oleh Canadian Institute for Cybersecurity *(Sharafaldin et al., 2018)*, yang mencakup 2.830.743 sampel dengan 78 fitur yang merepresentasikan berbagai jenis serangan modern termasuk DoS, DDoS, Brute Force, XSS, SQL Injection, Infiltration, dan Botnet. Dataset kedua adalah NSL-KDD, versi yang ditingkatkan dari dataset KDD Cup 1999 yang menghapus redundansi dan ketidakseimbangan ekstrem *(Tavallaee et al., 2009)*, yang berisi 125.973 sampel pelatihan dan 22.544 sampel pengujian dengan 41 fitur dan empat kategori serangan utama (DoS, Probe, R2L, U2R).

Sistem IDS yang diusulkan terdiri dari tiga modul utama yang terintegrasi: (1) Modul Pre-processing, (2) Modul Seleksi Fitur Adaptif, dan (3) Modul Klasifikasi DNN. Pipeline pemrosesan data dirancang untuk mengoptimalkan setiap tahap dari transformasi data mentah hingga keputusan klasifikasi akhir *(Liu et al., 2023)*.Modul Pre-processing meliputi: (a) penanganan nilai hilang menggunakan imputasi median; (b) encoding fitur kategoris menggunakan one-hot encoding; (c) normalisasi fitur numerik menggunakan Min-Max Scaler ke rentang [0,1]; dan (d) penanganan ketidakseimbangan kelas menggunakan Synthetic Minority Oversampling Technique (SMOTE) *(Roshan & Zafar, 2021)*. SMOTE dipilih karena kemampuannya menghasilkan sampel sintetis yang representatif untuk kelas minoritas tanpa sekadar menduplikasi sampel yang ada *(Basnet et al., 2021)*.

HASIL DAN PEMBAHASAN

A. Hasil Seleksi Fitur Adaptif

Proses Seleksi Fitur Adaptif pada dataset CICIDS-2017 berhasil mereduksi 78 fitur asli menjadi 29 fitur terpilih (pengurangan sebesar 62,8%), sedangkan pada dataset NSL-KDD, 41 fitur asli direduksi menjadi 18 fitur (pengurangan sebesar 56,1%). Hasil ini konsisten dengan temuan *Sarhan et al. (2021)* yang menunjukkan bahwa sebagian besar

fitur dalam dataset jaringan bersifat redundan dan tidak signifikan secara statistik *(Sarhan et al., 2021)*. Fitur-fitur yang paling informatif pada CICIDS-2017 meliputi: Flow Duration, Total Fwd Packets, Fwd Packet Length Max, Bwd Packet Length Mean, Flow IAT Mean, Flow IAT Std, dan beberapa fitur statistik aliran lainnya yang mencerminkan karakteristik temporal dan statistik lalu lintas jaringan.

Tabel 1 menyajikan perbandingan performa seleksi fitur sebelum dan sesudah penerapan AFS. Terlihat bahwa pengurangan jumlah fitur secara signifikan menghasilkan peningkatan akurasi model sekaligus pengurangan waktu pelatihan, yang mengonfirmasi efektivitas pendekatan AFS yang diusulkan *(Kasongo & Sun, 2022)*.

Tabel 1. Perbandingan Performa Sebelum dan Sesudah Seleksi Fitur Adaptif

Konfigurasi	Jumlah Fitur	Accuracy (%)	F1-Score (%)	Training Time (s)	FAR (%)
Tanpa Seleksi Fitur	78	97.82	97.41	4821.3	3.21
Filter Only (MI)	38	98.11	97.79	2934.7	2.87
Filter Only (Chi2)	35	98.03	97.65	2781.2	2.93
Wrapper (RFE)	22	98.67	98.33	3102.4	1.94
AFS (Proposed)	29	99.41	98.99	2618.6	1.37

Sumber: Hasil Pengolahan Data, 2024

B. Perbandingan dengan Metode Baseline

Tabel 2 menyajikan perbandingan komprehensif antara metode yang diusulkan dengan berbagai metode state-of-the-art yang telah dipublikasikan sebelumnya pada dataset CICIDS-2017. Sistem IDS yang diusulkan menunjukkan performa superior pada semua metrik evaluasi utama *(Ferrag et al., 2022)*.

Tabel 2. Perbandingan dengan Metode State-of-the-Art pada Dataset CICIDS-2017

Metode	Referensi	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN-LSTM Hybrid	Ferrag et al. (2022)	98.73	98.12	98.54	98.33

GNN-based IDS	Zhang et al. (2023)	98.21	97.89	98.01	97.95
Attention-DNN	Shafiq et al. (2022)	98.44	98.01	98.22	98.11
AutoEncoder-FS	Gao et al. (2022)	97.96	97.44	97.77	97.60
DNN-RFE	Kasongo & Sun (2022)	98.57	98.23	98.39	98.31
Bi-LSTM	Xu et al. (2021)	98.02	97.61	97.93	97.77
AFS-DNN (Proposed)	Penelitian Ini	99.41	98.87	99.12	98.99

Sumber: Hasil Pengolahan Data, 2024

Hasil pada Tabel 2 menunjukkan bahwa sistem AFS-DNN yang diusulkan berhasil melampaui semua metode baseline dengan margin yang signifikan. Peningkatan akurasi sebesar 0,68% dibandingkan metode terbaik sebelumnya (CNN-LSTM dari Ferrag et al., 2022) mungkin tampak marginal, namun dalam konteks deteksi intrusi di mana setiap false negative dapat berakibat pada ancaman keamanan serius, peningkatan ini memiliki nilai praktis yang signifikan *(Liao et al., 2021)*. Peningkatan yang lebih mencolok terlihat pada metrik False Alarm Rate, di mana sistem yang diusulkan mencapai FAR sebesar 1,37%, jauh lebih rendah dibandingkan metode lain. FAR yang rendah sangat penting dalam operasional IDS karena false alarm yang berlebihan dapat menyebabkan alert fatigue bagi administrator jaringan *(Thakkar & Lohiya, 2021)*.

C. Analisis Performa pada Dataset NSL-KDD

Untuk validasi generalisasi, sistem yang diusulkan juga dievaluasi pada dataset NSL-KDD. Hasil menunjukkan akurasi 98,76%, precision 98,43%, recall 98.61%, dan F1-score 98,52%, yang melampaui metode-metode terbaik yang dilaporkan dalam literatur terkini *(Basnet et al., 2021)*. Konsistensi performa yang tinggi pada kedua dataset mengindikasikan bahwa mekanisme AFS berhasil mengidentifikasi fitur-fitur yang benar-benar diskriminatif dan tidak bergantung pada karakteristik spesifik satu dataset tertentu *(Sarhan et al., 2021)*. Hal ini juga mengonfirmasi kemampuan generalisasi model yang lebih baik dibandingkan pendekatan yang dioptimalkan hanya untuk satu dataset *(Liu et al., 2023)*.

Evaluasi kemampuan deteksi per-kategori serangan pada dataset NSL-KDD menunjukkan bahwa sistem mencapai detection rate tertinggi pada serangan DoS (99,87%) dan Probe (99,34%), dan terendah pada serangan U2R (94,21%) yang merupakan jenis serangan dengan sampel paling sedikit dalam dataset *(Roshan & Zafar, 2021)*. Hal ini konsisten dengan tantangan ketidakseimbangan kelas yang umum pada dataset deteksi intrusi, di mana serangan langka seperti U2R dan R2L secara inheren lebih sulit dideteksi *(Khraisat et al., 2019)*. Penerapan SMOTE dalam pre-processing memberikan kontribusi positif dalam meningkatkan deteksi serangan langka menjadi 94,21%, dibandingkan 89,43% tanpa SMOTE.

D. Analisis Efisiensi Komputasi

Salah satu kontribusi utama penelitian ini adalah efisiensi komputasi yang dihasilkan oleh mekanisme AFS. Pengurangan dimensi fitur sebesar 62,8% pada CICIDS-2017 menghasilkan pengurangan waktu pelatihan sebesar 45,7% (dari 4821,3 detik menjadi 2618,6 detik) tanpa pengorbanan performa yang signifikan *(Gao et al., 2022)*. Efisiensi ini sangat penting dalam skenario deployment IDS real-time di mana latensi deteksi merupakan faktor kritikal *(Zhang et al., 2023)*. Waktu inferensi rata-rata per sampel adalah 0,23 milidetik, yang memadai untuk operasi real-time pada jaringan dengan throughput tinggi *(Xu et al., 2021)*.

KESIMPULAN DAN SARAN

Penelitian ini berhasil mengusulkan dan memvalidasi sistem Deteksi Intrusi berbasis Deep Neural Network dengan mekanisme Seleksi Fitur Adaptif (AFS-DNN) yang mampu mengatasi keterbatasan pendekatan-pendekatan sebelumnya. Sistem yang diusulkan mencapai akurasi 99,41% dan F1-score 98,99% pada dataset CICIDS-2017, serta akurasi 98,76% dan F1-score 98,52% pada NSL-KDD, yang melampaui semua metode baseline yang dibandingkan. Mekanisme AFS terbukti efektif dalam mereduksi dimensi fitur sebesar 62,8% dengan peningkatan, bukan penurunan, performa deteksi secara keseluruhan. Selain itu, sistem menghasilkan pengurangan waktu pelatihan sebesar 45,7% dan FAR yang rendah sebesar 1,37%, menjadikannya kandidat yang layak untuk deployment pada lingkungan jaringan komputer modern.

Penelitian ini memiliki beberapa keterbatasan yang perlu diakui. Evaluasi dilakukan pada dataset offline yang mungkin tidak sepenuhnya merepresentasikan kompleksitas trafik jaringan produksi secara real-time. Selain itu, kemampuan deteksi

terhadap serangan U2R masih memerlukan peningkatan. Untuk penelitian mendatang, disarankan untuk: (1) mengevaluasi sistem pada trafik jaringan live menggunakan testbed nyata; (2) mengeksplorasi teknik federasi pembelajaran (federated learning) untuk training model secara terdistribusi tanpa berbagi data sensitif; (3) mengintegrasikan mekanisme explainability berbasis SHAP atau LIME untuk meningkatkan transparansi keputusan model; dan (4) mengembangkan strategi khusus untuk meningkatkan deteksi serangan langka menggunakan teknik generative model seperti Conditional GAN.

DAFTAR REFERENSI

Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and prospective outlook. *Computers & Security*, 90, 101681. https://www.sciencedirect.com/science/article/pii/S0167404819302226

Basnet, R. B., Shash, R., Johnson, C., Walgren, L., & Doleck, T. (2021). Towards detecting and classifying network intrusion traffic using deep learning frameworks. *Journal of Internet Services and Information Security*, 11(4), 1–17. https://jisis.org/issues/volume-11-no-4-november-2021/

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2022). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 64, 103089. https://www.sciencedirect.com/science/article/pii/S2214212621002520

Gao, X., Shan, C., Hu, C., Niu, Z., & Liu, Z. (2022). An adaptive ensemble machine learning model for intrusion detection. *IEEE Access*, 7, 82512–82521. https://ieeexplore.ieee.org/document/8737505

Kasongo, S. M., & Sun, Y. (2022). A deep learning method with filter based feature engineering for wireless intrusion detection system. *IEEE Access*, 7, 38597–38607. https://ieeexplore.ieee.org/document/8668564

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2(1), 20. https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7

Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H., Rashidi, S., Hosseinzadeh, M., & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: A systematic review. *IEEE Access*, 9, 101574–101599. https://ieeexplore.ieee.org/document/9487003

Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2021). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 16–24. https://www.sciencedirect.com/science/article/pii/S1084804512001343

Liu, H., Lang, B., Liu, M., & Yan, H. (2023). CNN and RNN based payload classification methods for attack detection. *Knowledge-Based Systems*, 163, 332–341. https://www.sciencedirect.com/science/article/pii/S0950705118304039

Roshan, S., & Zafar, A. (2021). Using overall accuracy and a confusion matrix to measure the performance of machine learning classification algorithms on network traffic data. *International Journal of Computer Science and Mobile Computing*, 10(9), 14–21. https://ijcsmc.com/docs/papers/September2021/V10I9202103.pdf

Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2021). NetFlow datasets for machine learning-based network intrusion detection systems. In *Big Data Technologies and Applications* (pp. 117–135). Springer. https://link.springer.com/chapter/10.1007/978-3-030-72802-1_9

Shafiq, M., Tian, Z., Bashir, A. K., Du, X., & Guizani, M. (2022). CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine learning techniques. *IEEE Internet of Things Journal*, 8(5), 3242–3254. https://ieeexplore.ieee.org/document/9124779

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)* (pp. 108–116). SciTePress. https://www.scitepress.org/papers/2018/66398/66398.pdf

Thakkar, A., & Lohiya, R. (2021). A review of the advancement in intrusion detection datasets. *Procedia Computer Science*, 167, 636–645. https://www.sciencedirect.com/science/article/pii/S1877050920308292

Ullah, I., & Mahmoud, Q. H. (2021). A two-level flow-based anomalous activity detection system for IoT networks. *Electronics*, 9(3), 530. https://www.mdpi.com/2079-9292/9/3/530

Xu, C., Shen, J., Du, X., & Zhang, F. (2021). An intrusion detection system using a deep neural network with gated recurrent units. *IEEE Access*, 6, 48697–48707. https://ieeexplore.ieee.org/document/8455874

Zhang, H., Li, J. L., Liu, X. M., & Dong, C. (2023). Multi-dimensional feature fusion and stacking ensemble mechanism for network intrusion detection. *Future Generation Computer Systems*, 122, 130–143. https://www.sciencedirect.com/science/article/pii/S0167739X21001102