DAFTAR PUSTAKA

Albaseer A, Abdallah M. 2022. Fine-tuned LSTM-Based Model for Efficient Honeypot-Based Network Intrusion Detection System in Smart Grid Networks. Di dalam: *2022 5th International Conference on Communications, Signal Processing, and their Applications, ICCSPA 2022*. Institute of Electrical and Electronics Engineers Inc.

Arnob AKB, Mridha MF, Safran M, Amiruzzaman M, Islam MR. 2025. An Enhanced LSTM Approach for Detecting IoT-Based DDoS Attacks Using Honeypot Data. *International Journal of Computational Intelligence Systems*. 18(1). https://doi.org/10.1007/s44196-025-00741-7.

Bagui S, Li K. 2021. Resampling imbalanced data for network intrusion detection datasets. *J Big Data*. 8(1). https://doi.org/10.1186/s40537-020-00390-x.

Du M, Li F, Zheng G, Srikumar V. 2017. DeepLog: Anomaly detection and diagnosis from system logs through deep learning. Di dalam: *Proceedings of the ACM Conference on Computer and Communications Security*. Association for Computing Machinery. hlm 1285–1298.

Han J, Pak W. 2023. Hierarchical LSTM-Based Network Intrusion Detection System Using Hybrid Classification. *Applied Sciences (Switzerland)*. 13(5). https://doi.org/10.3390/app13053089.

Laghrissi FE, Douzi S, Douzi K, Hssina B. 2021. Intrusion detection systems using long short-term memory (LSTM). *J Big Data*. 8(1). https://doi.org/10.1186/s40537-021-00448-4.

Momand A, Jan SU, Ramzan N. 2023. A Systematic and Comprehensive Survey of Recent Advances in Intrusion Detection Systems Using Machine Learning: Deep Learning, Datasets, and Attack Taxonomy. *J Sens*. 2023. https://doi.org/10.1155/2023/6048087.

Sasse L, Nicolaisen-Sobesky E, Dukart J, Eickhoff SB, Götz M, Hamdan S, Komeyer V, Kulkarni A, Lahnakoski JM, Love BC, *et al*. 2025. Overview

of leakage scenarios in supervised machine learning. *J Big Data*. 12(1). https://doi.org/10.1186/s40537-025-01193-8.

Sewak M, Sahay SK, Rathore H. 2020 Des 26. Assessment of the Relative Importance of different hyper-parameters of LSTM for an IDS.

Saba T, Rehman A, Sadad T, Kolivand H, Bahaj SA. 2022. Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers & Electrical Engineering. 99. http://researchonline.ljmu.ac.uk/id/eprint/16451/.

Nurma A, Darmawan AS. 2023. Perancangan E-Library Berbasis Web Pada Sekolah Menengah Pertama. Jurnal Manajemen Pendidikan. 7(3). hlm 654–660. https://doi.org/10.36647/jmp.v7i3.14074.

Basuki BM, Cahyono D. 2025. Model Machine Learning SVM (Support Vector Machine) untuk Deteksi Anomali pada Sistem Kelistrikan Perusahaan Kerajinan Kayu GS4. Jurnal Teknik Mesin, Industri, Elektro dan Informatika. 4(1). hlm 310–320. https://doi.org/10.55606/jtmei.v4i1.4839.

Gusti KW. 2023. Perbandingan metode Support Vector Machine dan Logistic Regression untuk klasifikasi bencana alam. Informatik: Jurnal Ilmu Komputer. 19(2). hlm 134–140. https://doi.org/10.52958/iftk.v19i2.6355.

Prabuningrat GSW, Hostiadi DP, Srinadi NLP. 2024. Klasifikasi Deteksi Anomali Menggunakan Metode Machine Learning. Seminar Hasil Penelitian Informatika dan Komputer (SPINTER). 1(2). hlm 845–850. https://spinter.stikom-bali.ac.id/index.php/spinter/article/view/245.

Widianto MR, Suryanata MI, Arifin MD. 2024. Meningkatkan Keamanan Jaringan Dalam Pendekatan Terhadap Ancaman Siber Modern. Jurnal JIFORTY. 5(2). hlm 321–334. https://doi.org/10.30865/jiforty.v5i2.3453.

Maulani IE, Umam AF. 2023. Evaluasi efektivitas sistem deteksi intrusi dalam menjamin keamanan jaringan. Jurnal Sosial dan Teknologi. 3(8). hlm 662–667. https://doi.org/10.59188/jurnalsostech.v3i8.907.

Chen L, Li J. 2024. Advanced Preprocessing for Deep Learning in Network Security. Journal of Cyber Security and Mobility. 12(1). hlm 45–68.

Widodo AO, Setiawan B, Indraswari R. 2024. Machine Learning-Based Intrusion Detection on Multi-Class Imbalanced Dataset Using SMOTE. Procedia Computer Science. 234. hlm 578–583. https://doi.org/10.1016/j.procs.2024.03.042.

Parlika R, Afifudin M, Pradana IA, Wiratama YDW, Holis MN. 2023. Studi literatur efisiensi model rapid application development dalam pengembangan perangkat lunak (2014–2022). POSITIF: Jurnal Sistem Dan Teknologi Informasi. 8(2). hlm 64–73. https://doi.org/10.31961/positif.v8i2.1329.

Ali ML, Al-Amin M, Hossen MB, Islam MM, Moni MA, Islam MR. 2024. Deep Learning vs. Machine Learning for Intrusion Detection in Computer Networks: A Comparative Study. Applied Sciences. 15(4). https://doi.org/10.3390/app15041903.

Chawla A, et al. 2023. Framework for Machine Learning Model Deployment using Flask API. International Journal of Advanced Research in Computer Science. https://doi.org/10.26481/ijarcs.v14i2.7145.

Albaseer A, Abdallah M. 2022. Fine-tuned LSTM-Based Model for Efficient Honeypot-Based Network Intrusion Detection System in Smart Grid Networks. Di dalam: 2022 5th International Conference on Communications, Signal Processing, and their Applications, ICCSPA 2022. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCSPA55860.2022.10019245.

Praptodiyono S, Firmansyah T, Anwar MH, Wicaksana CA, Pramudyo AS, Al-Allawee A. 2023. Development of hybrid intrusion detection system based on suricata with pfsense method for highly reduction of DDoS attack on IPv6 networks. Eastern-European Journal of Enterprise Technologies. 5(9(125)). hlm 75–84. https://doi.org/10.15587/1729-4061.2023.285275.

Bhuiyan MZA, et al. 2023. NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning. Arabian Journal for Science and Engineering. https://doi.org/10.1016/j.ajic.2023.10.005.

Jayant P, Mohana, Shetty PM, Moharir M, Jeevan S, Kumar AR. 2023. Intrusion Detection in Network Traffic Using LSTM and Deep Learning. Di dalam: 2022 4th International Conference on Advances in Computing,

Communication Control and Networking, ICAC3N. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICAC3N56670.2022.10074251.

Setiawan I, Rochim AF, Martono KT. 2020. Performance Analysis of Intrusion Detection System (IDS) using Suricata and Snort on Private Cloud. Jurnal Teknologi dan Sistem Komputer. 8(2). hlm 115–121. https://doi.org/10.14710/jtsiskom.2020.13437.

Kokkali A, Sahni V. 2022. Network Intrusion Detection System using CNN-LSTM Hybrid Network. MSc Research Project. National College of Ireland. https://norma.ncirl.ie/6016/.

Bouke MA, Abdullah A. 2023. An empirical study of pattern leakage impact during data preprocessing on machine learning-based intrusion detection models reliability. Expert Systems with Applications. 230. 120715. https://doi.org/10.1016/j.eswa.2023.120715.

Du M, Li F, Zheng G, Srikumar V. 2017. DeepLog: Anomaly detection and diagnosis from system logs through deep learning. Di dalam: Proceedings of the ACM Conference on Computer and Communications Security. Association for Computing Machinery. hlm 1285–1298. https://doi.org/10.1145/3133956.3134015.

Scikit-learn. 2026. StandardScaler. Scikit-learn Documentation. https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.StandardScaler.html.

Cowrie. 2026. Cowrie SSH/Telnet Honeypot. GitHub. https://github.com/cowrie/cowrie.

Cowrie. 2026. Output Event Code Reference. Cowrie Documentation. https://docs.cowrie.org/en/latest/OUTPUT.html.