DAFTAR PUSTAKA

Aamir, M., & Zaidi, S. M. A. (2019). DDoS Attack Detection with feature engineering and machine learning: the framework and performance evaluation. *International Journal of Information Security*, *18*(6), 761–785. https://doi.org/10.1007/s10207-019-00434-1

Aleesa, A. M., Younis, M., Mohammed, A. A., & Sahar, N. M. (2021). Deep-Intrusion Detection System With Enhanced UNSW-NB15 Dataset Based On Deep Learning Techniques. In *Journal of Engineering Science and Technology* (Vol. 16, Issue 1)

Amrish, R., Bavapriyan, K., Gopinaath, V., Jawahar, A., & Vinoth Kumar, C. (2022). DDoS Detection using Machine Learning Techniques. *Journal of ISMAC*, *4*(1), 24–32. https://doi.org/10.36548/jismac.2022.1.003

Aqil, M., Azmi, H., Feresa, C., Foozy, M., Amin, K., Sukri, M., Abdullah, A., Rahmi, I., Hamid, A., & Amnur, H. (2021). Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms. *International Journal on Informatics Visualization*, 395–401. www.joiv.org/index.php/joiv

Aurélien Géron. (2023). *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, 3rd Edition* (N. Butterfield, N. Tache, M. Cronin, B. Kelly, & K. Cofer, Eds.; 3rd ed.). O'Reilly Media Inc.

Faiz, M. N., Somantri, O., & Muhammad, A. W. (2022). Rekayasa Fitur Berbasis Machine Learning untuk Mendeteksi Serangan DDoS. In *Jurnal Nasional Teknik Elektro dan Teknologi Informasi* | (Vol. 11, Issue 3).

Fitzgerald, K., Browne, L. M., & Butler, R. F. (2019). Using the Agile software development lifecycle to develop a standalone application for generating colour magnitude diagrams. *Astronomy and Computing*, *28*. https://doi.org/10.1016/j.ascom.2019.05.001

Habeeb, M. S., & Ranga Babu, T. (2024). Two-Phase Feature Selection Technique using Information Gain and XGBoost-RFE for NIDS. *International Journal of Intelligent Systems and Applications in Engineering A T*, *2024*(13s), 278–287. https://orcid.org/0000-0002-4946-1452

Kasongo, S. M., & Sun, Y. (2020a). Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-020-00379-6

Maslan, A., Mohamad, K. M. Bin, & Mohd Foozy, F. B. (2020). Feature selection for DDoS detection using classification machine learning techniques. *IAES International Journal of Artificial Intelligence*, *9*(1), 137–145. https://doi.org/10.11591/ijai.v9.i1.pp137-145

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*. https://doi.org/10.1109/MILCIS.2015.7348942

Nimbalkar, P., & Kshirsagar, D. (2021b). Feature selection for intrusion detection system in Internet-of-Things (IoT). *ICT Express*, *7*(2), 177–181. https://doi.org/10.1016/j.icte.2021.04.012

Prasetiyowati, M. I., Maulidevi, N. U., & Surendro, K. (2021). Determining threshold value on information gain feature selection to increase speed and prediction accuracy of random forest. *Journal of Big Data*, *8*(1). https://doi.org/10.1186/s40537-021-00472-4

Real-Time Systems: Design Principles for Distributed Embedded Applications - Hermann Kopetz, Wilfried Steiner - Google Books. (n.d.). Retrieved January 6, 2025, from https://books.google.co.id/books?hl=en&lr=&id=36iLEAAAQBAJ&oi=fnd&pg=PR5&dq=real+time+applications&ots=riWRVy0T_S&sig=6d7uIyQWFfzwa9LwBFJPWxAILAk&redir_esc=y#v=onepage&q=real%20time%20applications&f=false

Saied, A., Overill, R. E., & Radzik, T. (2016). Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing*, *172*, 385–393. https://doi.org/10.1016/j.neucom.2015.04.101

Sambangi, S., & Gondi, L. (2020). *A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression*. 51. https://doi.org/10.3390/proceedings2020063051

Somani, G., Singh Gaur, M., & Conti, M. (n.d.). *Combating DDoS Attacks in the Cloud: Requirements, Trends, and Future Directions*.

Tuan, T. A., Long, H. V., Son, L. H., Kumar, R., Priyadarshini, I., & Son, N. T. K. (2020). Performance evaluation of Botnet DDoS attack detection using machine learning. *Evolutionary Intelligence*, *13*(2), 283–294. https://doi.org/10.1007/S12065-019-00310-W/METRICS

Jacob, P. M., & Prasanna, M. (2016). A Comparative analysis on Black box testing strategies. 2016 International Conference on Information Science (ICIS). doi:10.1109/infosci.2016.7845290