DAFTAR PUSTAKA

Arief, M., Hari Trisnawan, P., & Data, M. (2017). *IMPLEMENTASI SISTEM DETEKSI SERANGAN SLOWLORIS PADA ARSITEKTUR JARINGAN SOFTWARE-DEFINED NETWORK MENGGUNAKAN RANDOM FOREST* (Vol. 1, Issue 1). http://j-ptiik.ub.ac.id

Dhaliwal, A. S. (2017). *Detection and Mitigation of SYN and HTTP flood DDoS attacks in Software Defined Networks*.

Haeruddin, H., Erick, E., & Aripradono, H. W. (2025). Perbandingan Support Vector Machine, Random Forest Classifier, dan K-Nearest Neighbour dalam Pendeteksian Anomali pada Jaringan DDos. *JTIM : Jurnal Teknologi Informasi Dan Multimedia*, *7*(1), 23–33. https://doi.org/10.35746/jtim.v7i1.628

He, J., Fang, W., Lan, X., Yang, G., Chen, Z., Chen, Y., Li, T., & Chen, J. (2024). Efficient Based on Improved Random Forest Defense System Against Application-Layer DDoS Attacks. *International Journal of Intelligent Systems*, *2024*(1). https://doi.org/10.1155/2024/9044391

Islam, M. M., Shahid, S., Awar, K. B., Khan, R., & Sohail, M. (2021). Cyber-Security: Dos Attack Outcomes are Dangerous. *European Journal of Electrical Engineering and Computer Science*, *5*(3), 54–59.

Jairu, P., & Mailewa, A. B. (2022). Network Anomaly Uncovering on CICIDS-2017 Dataset: A Supervised Artificial Intelligence Approach. *IEEE International Conference on Electro Information Technology*, *2022-May*, 606–615. https://doi.org/10.1109/eIT53891.2022.9814045

Laiq, F., Al-Obeidat, F., Amin, A., & Moreira, F. (2023). DDoS Attack Detection in Edge-IIoT using Ensemble Learning. *2023 7th Cyber Security in Networking Conference, CSNet 2023*, 204–207. https://doi.org/10.1109/CSNet59123.2023.10339784

Naveen Bindra, & Manu Sood. (2019). Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset. *Automatic Control and Computer Sciences*, *53*(5), 419–428. https://doi.org/10.3103/S0146411619050043

Sanmorino, A., Marnisah, L., & Di Kesuma, H. (2024). Detection of DDoS Attacks using Fine-Tuned Multi-Layer Perceptron Models. *Engineering, Technology and Applied Science Research*, *14*(5), 16444–16449. https://doi.org/10.48084/etasr.8362