Daftar Pustaka

Abu Al-Haija, Q. and Al-Dala'ien, M. (2022), 'Elba-iot: An ensemble learning model for botnet attack detection in iot networks', *Journal of Sensor and Actuator Networks* **11**(1).
URL: *https://www.mdpi.com/2224-2708/11/1/18*

Alhowaide, A., Alsmadi, I. and Tang, J. (2021), 'Ensemble detection model for iot ids', *Internet of Things* **16**, 100435.
URL: *https://www.sciencedirect.com/science/article/pii/S2542660521000792*

Alissa, K., Alyas, T., Zafar, K., Abbas, Q., Tabassum, N. and Sakib, S. (2022), 'Botnet attack detection in iot using machine learning', *Computational In- telligence and Neuroscience* **2022**, 4515642.
URL: *https://doi.org/10.1155/2022/4515642*

Antonakakis, M. (2017), 'Understanding the mirai botnet', *USENIX* p. 1093–1110.

Arshad, A., Jabeen, M., Ubaid, S., Raza, A., Abualigah, L., Aldiabat, K. and Jia, H. (2023), 'A novel ensemble method for enhancing internet of things device security against botnet attacks', *Decision Analytics Journal* **8**, 100307.
URL: *https://www.sciencedirect.com/science/article/pii/S2772662223001479*

Cao, Y., Wang, Z., Ding, H., Zhang, J. and Li, B. (2024), Iot botnet attacks detection and classification based on ensemble learning, *in* H. Lu and J. Cai, eds, 'Artificial Intelligence and Robotics', Springer Nature Singapore, Singa- pore, pp. 45–55.

Dey, A. K., Gupta, G. P. and Sahu, S. P. (2023), 'A metaheuristic-based ensemble feature selection framework for cyber threat detection in iot-enabled networks', *Decision Analytics Journal* **7**, 100206.
URL: *https://www.sciencedirect.com/science/article/pii/S2772662223000462*

Hossain, M. A. and Islam, M. S. (2023), 'Ensuring network security with a robust intrusion detection system using ensemble-based machine learning', *Array* **19**, 100306.
URL: *https://www.sciencedirect.com/science/article/pii/S2590005623000310*

Jiyeon Kim, Minsun Shim, S. H. Y. S. . and Choi, E. (2020), 'Intelligent detection of iot botnets using machine learning and deep learning', *Applied Sciences* **10**, 7009.

Lakshmanan, R. (n.d.), 'New mirai variant and zhtrap botnet malware emerge in the wild', *The Hacker News* .
URL: *https://thehackernews.com/2021/03/new-mirai-variant-and-zhtrap-botnet.html*

Lazzarini, R., Tianfield, H. and Charissis, V. (2023), 'A stacking ensemble of deep learning models for iot intrusion detection', *Knowledge-Based Systems* **279**, 110941.
URL: *https://www.sciencedirect.com/science/article/pii/S0950705123006913*

Louk, M. H. L. and Tama, B. A. (2023), 'Dual-ids: A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system', *Expert Systems with Applications* **213**, 119030.
URL: *https://www.sciencedirect.com/science/article/pii/S0957417422020486*

Mirsky, Y., Doitshman, T., Elovici, Y. and Shabtai, A. (2018), 'Kitsune: An ensemble of autoencoders for online network intrusion detection', *CoRR* **abs/1802.09089**.
URL: *http://arxiv.org/abs/1802.09089*

Padhiar, S. and Patel, R. (2023), 'Performance evaluation of botnet detection using machine learning techniques', *International Journal of Electrical and Computer Engineering (IJECE)* **13**, 6827.

Pokhrel, S., Abbas, R. and Aryal, B. (2021), 'Iot security: Botnet detection iniot using machine learning', *CoRR* **abs/2104.02231**.
URL: *https://arxiv.org/abs/2104.02231*

Rezaei, A. (2021), 'Using ensemble learning technique for detecting botnet on iot', *SN Computer Science* **2**(3), 148.
URL: *https://doi.org/10.1007/s42979-021-00585-w*

Srinivasan, S. and P, D. (2023), 'Enhancing the security in cyber-world by detecting the botnets using ensemble classification based machine learning', *Measurement: Sensors* **25**, 100624.
URL: *https://www.sciencedirect.com/science/article/pii/S2665917422002586*

UNTERFINGHER, V. (n.d.), 'A technical analysis of the mirai botnet phenomenon', *Heimdal Security Blog* .
URL: *https://heimdalsecurity.com/blog/mirai-botnet-phenomenon/*

Yang, L. and Shami, A. (2022), ‘Ids-ml: An open source code for intrusion detection system development using machine learning’, *Software Impacts* **14**, 100446.
URL: *https://www.sciencedirect.com/science/article/pii/S2665963822001300*