

Daftar Pustaka

- [1] R. Kalakoti, H. Bahsi, and S. Nomm, "Improving IoT security with explainable AI: Quantitative evaluation of explainability for IoT botnet detection," *IEEE Internet of Things Journal*, 2024.
- [2] A. A. Wardana and P. Sukarno, "Taxonomy and Survey of Collaborative Intrusion Detection System using Federated Learning," *ACM Computing Surveys*, vol. 57, no. 4, pp. 1–36, 2024.
- [3] M. Fazzolari, P. Ducange, and F. Marcelloni, "An explainable intrusion detection system for IoT networks," in *2023 IEEE International Conference on Fuzzy Systems (FUZZ)*, pp. 1–6, IEEE, 2023.
- [4] R. Kumar, A. Aljuhani, D. Javeed, P. Kumar, S. Islam, and A. K. M. N. Islam, "Digital twins-enabled zero-touch network: A smart contract and explainable AI integrated cybersecurity framework," *Future Generation Computer Systems*, 2024.
- [5] A. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.
- [6] R. Kalakoti, S. Nomm, and H. Bahsi, "Improving transparency and explainability of deep learning-based IoT botnet detection using explainable artificial intelligence (XAI)," in *2023 International Conference on Machine Learning and Applications (ICMLA)*, pp. 595–601, IEEE, 2023.
- [7] P. H. Do, T. D. Le, V. Vishnevsky, A. Berezkin, and R. Kirichek, "A horizontal federated learning approach to IoT malware traffic detection: An empirical evaluation with N-BaIoT dataset," in *2024 26th International Conference on Advanced Communications Technology (ICACT)*, pp. 1494–1506, IEEE, 2024.
- [8] M. Alqahtani, H. Mathkour, and M. M. B. Ismail, "IoT botnet attack detection based on optimized extreme gradient boosting and feature selection," *Sensors*, vol. 20, no. 21, p. 6336, 2020.
- [9] R. K. Sevakula and N. K. Verma, "Assessing generalization ability of majority vote point classifiers," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 28, no. 12, pp. 2985–2997, 2016.
- [10] H. Li, et al., "Ensemble learning for overall power conversion efficiency of the all-organic dye-sensitized solar cells," *IEEE Access*, vol. 6, pp. 34118–34126, 2018.
- [11] I. D. Mienye, Y. Sun, and Z. Wang, "An improved ensemble learning approach for the prediction of heart disease risk," *Informatics in Medicine Unlocked*, vol. 20, p. 100402, 2020.
- [12] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, "CatBoost: Unbiased boosting with categorical features," in *Advances in Neural Information Processing Systems*, pp. 6638–6648, 2018.
- [13] R. Sanjeetha, A. Raj, K. Saivenu, M. I. Ahmed, B. Sathvik, and A. Kanavalli, "Detection and mitigation of botnet-based DDoS attacks using CatBoost machine learning algorithm in SDN environment," *International Journal of Advanced Technology and Engineering Exploration*, vol. 8, no. 76, p. 445, 2021.
- [14] J. Zeng, M. Zhang, and S.-B. Lin, "Fully corrective gradient boosting with squared hinge: Fast learning rates and early stopping," *Neural Networks*, vol. 147, pp. 136–151, 2022.
- [15] T. Zhang and B. Yu, "Boosting with early stopping: Convergence and consistency," 2005.
- [16] A. A. Wardana, G. Kołaczek, A. Warzynski, and P. Sukarno, "Ensemble averaging deep neural network for botnet detection in heterogeneous Internet of Things devices," *Scientific Reports*, vol. 14, no. 1, pp. 3878, 2024.