Daftar Pustaka

[1] Tie Qiu, Jiancheng Chi, Xiaobo Zhou, Zhaolong Ning, Mohammed Atiquzzaman, and Dapeng Oliver Wu, Edge computing in industrial internet of things: Architecture, advances and challenges, IEEE Com munications Surveys & Tutorials, vol. 22, no. 4, pp. 2462–2488, 2020.

[2] Fazlullah Khan, Mian Ahmad Jan, Ateeq ur Rehman, Spyridon Mas torakis, Mamoun Alazab, and Paul Watters, A secured and intelligent communication scheme for iiot-enabled pervasive edge computing, IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 5128–5137, 2020.

[3] A. A. Wardana, P. Sukarno, S. Basuki, and S. B. Utomo, ”Federated Random Forest with Feature Selection for Collaborative Intrusion Detection in Internet of Things,” Procedia Computer Science, vol. 246, pp. 20-29, 2024, 28th International Conference on Knowledge Based and Intelligent Information and Engineering Systems (KES 2024), doi: 10.1016/j.procs.2024.09.193.

[4] M. R. Rawadi H, P. Sukarno, and A. A. Wardana, ”Performance Anal ysis of Deep Neural Decision Forest with Extratrees Feature Selection for Obfuscated Malware Detection,” 2024 IEEE 3rd International Con ference on Computing and Machine Intelligence (ICMI), Mt Pleasant, MI, USA, 2024, pp. 1-5, doi: 10.1109/ICMI60790.2024.10586174.

[5] Juan Vanerio and Pedro Casas, Ensemble-learning approaches for network security and anomaly detection, Proceedings of the Workshop on Big Data Analytics and Machine Learning for Data Communication Networks, pp. 1–6, 2017.

[6] Nicholas Jeffrey, Qing Tan, and Jos´e R Villar, Using ensemble learning for anomaly detection in cyber–physical systems, Electronics, vol. 13, no. 7, pp. 1391, 2024.

[7] Jadel Alsamiri and Khalid Alsubhi, Internet of things cyber attacks detection using machine learning, International Journal of Advanced Computer Science and Applications, vol. 10, no. 12, 2019.

[8] Mahamdu Hasan, Md Milon, Md Ishrak Islam Zarif, and Hashem, Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches, Internet of Things, vol. 7, pp. 100059, 2019.

[9] Maryam Anwer, S Mahmood Khan, M Umer Farooq, et al., Attack detection in IoT using machine learning, Engineering, Technology & Applied Science Research, vol. 11, no. 3, pp. 7273–7278, 2021.

[10] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, ”Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning,” in IEEE Access, vol. 10, pp. 40281-40306, 2022, doi: 10.1109/AC CESS.2022.3165809.

[11] L. Breiman, ”Random Forests,” Machine Learning, vol. 45, no. 1, pp. 5-32, 2001, doi: 10.1023/A:1010933404324.

[12] T. Chen and C. Guestrin, XGBoost: A Scalable Tree Boosting Sys tem, Proceedings of the 22nd ACM SIGKDD International Confer ence on Knowledge Discovery and Data Mining, pp. 785–794, 2016. doi:10.1145/2939672.2939785

[13] S. J. Rigatti, Random Forest, J. Insur. Med., vol. 47, no. 1, pp. 31–39, 2017. doi:10.17849/insm-47-01-31-39.1

[14] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T.-Y. Liu, LightGBM: A Highly Efficient Gradient Boosting Decision Tree, Proceedings of the Neural Information Processing Systems, 2017. https://api.semanticscholar.org/CorpusID:3815895

[15] H. Braganc¸a, V. Rocha, E. Souto, D. Kreutz, and E. Feitosa, Explaining the Effectiveness of Machine Learning in Malware Detection: Insights from Explainable AI, Anais do XXIII Simp´osio Brasileiro de Seguranc¸a da Informac¸˜ao e de Sistemas Computacionais (SBSeg 2023), Brasil: Sociedade Brasileira de Computac¸˜ ao-SBC, Sep. 2023, pp. 181–194. doi: https://doi.org/10.5753/sbseg.2023.233595.

[16] Amal A Alahmadi, Malak Aljabri, Fahd Alhaidari, Danyah J Alharthi, Ghadi E Rayani, Leena A Marghalani, Ohoud B Alotaibi, and Shurooq A Bajandouh, DDoS attack detection in IoT-based networks using ma chine learning models: A survey and research directions, Electronics, vol. 12, no. 14, pp. 3103, 2023.

[17] Avish Karmakar, Naiwrita Dey, Tapadyuti Baral, Manojeet Chowd hury, and Md Rehan, Industrial internet of things: A review, 2019 International Conference on Opto-electronics and Applied Optics (OP TRONIX), pp. 1–6, 2019.

[18] Mouaad Mohy-eddine, Azidine Guezzaz, Said Benkirane, and Mourade Azrour, An effective intrusion detection approach based on ensemble learning for IIoT edge computing, Journal of Computer Virology and Hacking Techniques, vol. 19, no. 4, pp. 469–481, 2023.

[19] Alaa Alhowaide, Izzat Alsmadi, and Jian Tang, Ensemble detection model for IoT IDS, Internet of Things, vol. 16, pp. 100435, 2021.
[20] Vikas Tomer and Sachin Sharma, Detecting IoT attacks using an ensemble machine learning model, Future Internet, vol. 14, no. 4, pp. 102, 2022.
[21] David Gunning and David Aha, DARPA's Explainable Artificial Intel ligence (XAI) Program, AI Magazine, vol. 40, no. 2, pp. 44–58, 2019.
[22] Thi-Thu-Huong Le, Haeyoung Kim, Hyoeun Kang, and Howon Kim, Classification and explanation for intrusion detection system based on ensemble trees and SHAP method, Sensors, vol. 22, no. 3, pp. 1154, 2022