DAFTAR PUSTAKA

[1] E. N. Ylmaz, B. Ciylan, S. Gonen, E. Sindiren, and G. Karacayilmaz, "Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect," in *2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*, Istanbul, Turkey: IEEE, Apr. 2018, pp. 81–85. doi: 10.1109/SGCF.2018.8408947.

[2] I. Erkek and E. Irmak, "Cyber Security of Internet Connected ICS/SCADA Devices and Services," in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, Ankara, Turkey: IEEE, Dec. 2021, pp. 75–80. doi: 10.1109/ISCTURKEY53027.2021.9654285.

[3] T. Alladi, V. Chamola, and S. Zeadally, "Industrial Control Systems: Cyberattack trends and countermeasures," *Comput. Commun.*, vol. 155, pp. 1–8, Apr. 2020, doi: 10.1016/j.comcom.2020.03.007.

[4] "Serangan siber meluas ke industri otomatisasi - ANTARA News." Accessed: Apr. 05, 2025. [Online]. Available: https://www.antaranews.com/berita/2212450/serangan-siber-meluas-ke-industri-otomatisasi

[5] T. Hu, B. Liu, and J. Chen, "A Watermark Detection Method for Approximate Replay Attacks Based on State Compensation," in *2023 China Automation Congress (CAC)*, Chongqing, China: IEEE, Nov. 2023, pp. 3143–3147. doi: 10.1109/CAC59555.2023.10451608.

[6] M. Niedermaier, J.-O. Malchow, F. Fischer, D. Marzin, D. Merli, and V. Roth, "You Snooze, You Lose: Measuring PLC Cycle Times under Attacks".

[7] "Israel's largest oil refinery website offline after DDoS attack." Accessed: Apr. 05, 2025. [Online]. Available: https://www.bleepingcomputer.com/news/security/israels-largest-oil-refinery-website-offline-after-ddos-attack/

[8] "Cybersecurity: The key lessons of the Triton malware cyberattack you need to learn," ZDNET. Accessed: Apr. 05, 2025. [Online]. Available: https://www.zdnet.com/article/cybersecurity-the-key-lessons-of-the-triton-malware-cyberattack-you-need-to-learn/

[9] lalelong, "Industroyer 2 : the Russian Cyberattack on Ukraine Infrastructure," Headmind Partners. Accessed: Apr. 05, 2025. [Online]. Available: https://www.headmind.com/industroyer-2/

[10] E. Kovacs, "Severe DoS Flaw Discovered in Siemens SIMATIC PLCs," SecurityWeek. Accessed: Apr. 05, 2025. [Online]. Available: https://www.securityweek.com/severe-dos-flaw-discovered-siemens-simatic-plcs/

[11] P. Wasnik and N. Chavhan, "A Review Paper on Designing Intelligent Intrusion Detection System Using Deep Learning," in *2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP)*, Nagpur, India: IEEE, Apr. 2023, pp. 1–6. doi: 10.1109/ICETET-SIP58143.2023.10151563.

[12] R. Rai, M. K. Tiwari, D. Ivanov, and A. Dolgui, "Machine learning in manufacturing and industry 4.0 applications," *Int. J. Prod. Res.*, vol. 59, no. 16, pp. 4773–4778, Aug. 2021, doi: 10.1080/00207543.2021.1956675.
[13] R. K. Chouhan, M. Atulkar, and N. K. Nagwani, "A Centralized LGBM based Attack Detection and Mitigation Approach for Software Defined Networks," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India: IEEE, Jul. 2023, pp. 1–7. doi: 10.1109/ICCCNT56998.2023.10307092.
[14] P. Chauhan and M. Atulkar, "An efficient LGBM based DDoS attack Detection Approach for SD-IoT," in *2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Bhopal, India: IEEE, Feb. 2023, pp. 1–10. doi: 10.1109/SCEECS57921.2023.10063003.
[15] I. Kiss, P. Haller, and A. Bereş, "Denial of Service Attack Detection in Case of Tennessee Eastman Challenge Process," *Procedia Technol.*, vol. 19, pp. 835–841, 2015, doi: 10.1016/j.protcy.2015.02.120.
[16] C. Wang, B. Wang, H. Liu, and H. Qu, "Anomaly Detection for Industrial Control System Based on Autoencoder Neural Network," *Wirel. Commun. Mob. Comput.*, vol. 2020, pp. 1–10, Aug. 2020, doi: 10.1155/2020/8897926.
[17] P. Filonov, F. Kitashov, and A. Lavrentyev, "RNN-based Early Cyber-Attack Detection for the Tennessee Eastman Process," Sep. 07, 2017, *arXiv*: arXiv:1709.02232. doi: 10.48550/arXiv.1709.02232.
[18] S. Gargoum, N. Yassaie, A. W. Al-Dabbagh, and C. Feng, "A Data-Driven Framework for Verified Detection of Replay Attacks on Industrial Control Systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 3400–3415, 2025, doi: 10.1109/TASE.2024.3394315.
[19] S. Cui and D. Feng, "An Improved Support Vector Machine Attack Detection Algorithm for Industry Controls System," in *2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA)*, Jan. 2023, pp. 114–119. doi: 10.1109/ICPECA56706.2023.10076096.
[20] S. Sen and L. Song, "An IIoT-Based Networked Industrial Control System Architecture to Secure Industrial Applications," in *2021 IEEE Industrial Electronics and Applications Conference (IEACon)*, Penang, Malaysia: IEEE, Nov. 2021, pp. 280–285. doi: 10.1109/IEACon51066.2021.9654520.
[21] W. Oñate and R. Sanz, "Analysis of architectures implemented for IIoT," *Heliyon*, vol. 9, no. 1, Jan. 2023, doi: 10.1016/j.heliyon.2023.e12868.
[22] M. Krotofil, "Security of cyber-physical systems: process-aware approach," 2023, doi: 10.15480/882.4913.
[23] Krotofil, Marina and Larsen, Jason, *Rocking the pocket book: Hacking chemical plants*. in DefCon Conference, DEFCON. 2015.
[24] M. Doostmohammadian and N. Meskin, "Finite-Time Stability Under Denial of Service," *IEEE Syst. J.*, vol. 15, no. 1, pp. 1048–1055, Mar. 2021, doi: 10.1109/JSYST.2020.2992702.
[25] N. Lawrence Ricker, "Decentralized control of the Tennessee Eastman Challenge Process," *J. Process Control*, vol. 6, no. 4, pp. 205–221, Aug. 1996, doi: 10.1016/0959-1524(96)00031-5.

[26] B. Md. Irfan, V. Poornima, S. Mohana Kumar, U. S. Aswal, N. Krishnamoorthy, and R. Maranan, "Machine Learning Algorithms for Intrusion Detection Performance Evaluation and Comparative Analysis," in *2023 4th International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India: IEEE, Sep. 2023, pp. 01–05. doi: 10.1109/ICOSEC58147.2023.10275831.

[27] K. R. Dalal, "Analysing the Role of Supervised and Unsupervised Machine Learning in IoT," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Coimbatore, India: IEEE, Jul. 2020, pp. 75–79. doi: 10.1109/ICESC48915.2020.9155761.

[28] R. N. Thomas and R. Gupta, "A Survey on Machine Learning Approaches and Its Techniques:," in *2020 IEEE International Students' Conference on Electrical,Electronics and Computer Science (SCEECS)*, Bhopal, India: IEEE, Feb. 2020, pp. 1–6. doi: 10.1109/SCEECS48394.2020.190.

[29] A. A. Khan, O. Chaudhari, and R. Chandra, "A review of ensemble learning and data augmentation models for class imbalanced problems: Combination, implementation and evaluation," *Expert Syst. Appl.*, vol. 244, p. 122778, Jun. 2024, doi: 10.1016/j.eswa.2023.122778.

[30] N. H. PhD, "Mastering Ensemble Learning Techniques: Fundamentals, Algorithms, and Practical Applications," Medium. Accessed: Apr. 01, 2025. [Online]. Available: https://medium.com/@HalderNilimesh/mastering-ensemble-learning-techniques-fundamentals-algorithms-and-practical-applications-21a4fe95305c

[31] L. Yunhan, "Aviation Safety Ensemble Classification Model Based on Imbalanced Data," in *2023 XX Technical Scientific Conference on Aviation Dedicated to the Memory of N.E. Zhukovsky (TSCZh)*, Moscow, Russian Federation: IEEE, Apr. 2023, pp. 55–59. doi: 10.1109/TSCZh58792.2023.10233447.

[32] N. Talkhi *et al.*, "Prediction of serum anti-HSP27 antibody titers changes using a light gradient boosting machine (LightGBM) technique," *Sci. Rep.*, vol. 13, Aug. 2023, doi: 10.1038/s41598-023-39724-z.

[33] F. Meng, Y. Fu, F. Lou, and Z. Chen, "An Effective Network Attack Detection Method Based on Kernel PCA and LSTM-RNN," in *2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)*, Dalian: IEEE, Dec. 2017, pp. 568–572. doi: 10.1109/ICCSEC.2017.8447022.

[34] C. Ma, J. Zhang, L. Wang, and H. You, "Network Attack Detection Based on Kernel Principal Component Analysis and Decision Tree," in *2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Chongqing, China: IEEE, Oct. 2020, pp. 84–91. doi: 10.1109/CyberC49757.2020.00023.

[35] M. Lovrić, M. Milanović, and M. Stamenković, "Algoritmic methods for segmentation of time series: An overview".

[36] L. Guo and Y. Wei, "A Time Series Segment Finding Motifs Based On Sliding Window Algorithm," in *2024 IEEE International Conference on Industrial Technology (ICIT)*, Bristol, United Kingdom: IEEE, Mar. 2024, pp. 1–6. doi: 10.1109/ICIT58233.2024.10540977.

[37] C. Aldrich, "Process Fault Diagnosis for Continuous Dynamic Systems Over Multivariate Time Series," in *Time Series Analysis - Data, Methods, and Applications*, C.-K. Ngan, Ed., IntechOpen, 2019. doi: 10.5772/intechopen.85456.

[38] Q. Wang, B. Yan, H. Su, and H. Zheng, "Anomaly Detection for Time Series Data Stream," in *2021 IEEE 6th International Conference on Big Data Analytics (ICBDA)*, Xiamen, China: IEEE, Mar. 2021, pp. 118–122. doi: 10.1109/ICBDA51983.2021.9402957.

[39] M. Barandas *et al.*, "TSFEL: Time Series Feature Extraction Library," *SoftwareX*, vol. 11, p. 100456, Jan. 2020, doi: 10.1016/j.softx.2020.100456.

[40] Md. T. Uddin and Md. A. Uddiny, "A guided random forest based feature selection approach for activity recognition," in *2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, May 2015, pp. 1–6. doi: 10.1109/ICEEICT.2015.7307376.

[41] E. Elgeldawi, A. Sayed, A. R. Galal, and A. M. Zaki, "Hyperparameter Tuning for Machine Learning Algorithms Used for Arabic Sentiment Analysis," *Informatics*, vol. 8, no. 4, p. 79, Nov. 2021, doi: 10.3390/informatics8040079.

[42] I. Muhamad Malik Matin, "Hyperparameter Tuning Menggunakan GridsearchCV pada Random Forest untuk Deteksi Malware," *MULTINETICS*, vol. 9, no. 1, pp. 43–50, May 2023, doi: 10.32722/multinetics.v9i1.5578.

[43] Z. M. Alhakeem, Y. M. Jebur, S. N. Henedy, H. Imran, L. F. A. Bernardo, and H. M. Hussein, "Prediction of Ecofriendly Concrete Compressive Strength Using Gradient Boosting Regression Tree Combined with GridSearchCV Hyperparameter-Optimization Techniques," *Materials*, vol. 15, no. 21, p. 7432, Oct. 2022, doi: 10.3390/ma15217432.

[44] A. Subasi, *Practical machine learning for data analysis using Python*. London San Diego, CA Cambridge, MA Kidlington, Oxford: Academic Press, an imprint of Elsevier, 2020.

[45] A. Robles-Durazno, N. Moradpoor, J. McWhinnie, G. Russell, and I. Maneru-Marin, "PLC memory attack detection and response in a clean water supply system," *Int. J. Crit. Infrastruct. Prot.*, vol. 26, p. 100300, Sep. 2019, doi: 10.1016/j.ijcip.2019.05.003.

[46] jojeck, "Answer to 'STFT: why overlapping the window?,'" Signal Processing Stack Exchange. Accessed: Mar. 05, 2025. [Online]. Available: https://dsp.stackexchange.com/a/19317

[47] "Kernel PCA," scikit-learn. Accessed: Mar. 05, 2025. [Online]. Available: https://scikit-learn/stable/auto_examples/decomposition/plot_kernel_pca.html

[48] J. Yu, C. Xia, J. Xie, and H. Zhang, "Research on Feature Importance of Gait Mechanomyography Signal Based on Random Forest," in *2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL)*, Chongqing, China: IEEE, Jul. 2020, pp. 191–196. doi: 10.1109/CVIDL51233.2020.00045.