DAFTAR PUSTAKA

[1] H. R. Ghaeini and N. O. Tippenhauer, "HAMIDS: Hierarchical Monitoring Intrusion Detection System for Industrial Control Systems," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, Vienna Austria: ACM, Oct. 2016, pp. 103–111. doi: 10.1145/2994487.2994492.

[2] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, "Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks," *Appl. Soft Comput.*, vol. 71, pp. 66–77, Oct. 2018, doi: 10.1016/j.asoc.2018.06.017.

[3] Y. Gu, C. Hu, Y. Li, Y. Zhao, Q. Cui, and Y. Xie, "Design concept of intelligent integrated control system for neutral beam injection," *Plasma Phys. Control. Fusion*, vol. 66, no. 10, p. 105011, Oct. 2024, doi: 10.1088/1361-6587/ad731a.

[4] R. Luis de Moura, V. N. L. Franqueira, and G. Pessin, "Cybersecurity in Industrial Networks: Artificial Intelligence Techniques Applied to Intrusion Detection Systems," in *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*, Jul. 2023, pp. 2235–2242. doi: 10.1109/CSCE60160.2023.00365.

[5] R. Langner, "To Kill a Centrifuge A Technical Analysis of What Stuxnet ' s Creators Tried to Achieve," 2013. [*Online*]. Available: https://api.semanticscholar.org/CorpusID:14733319

[6] K. Zetter, "A cyberattack has caused confirmed physical damage for the second time ever," *WIRED*, 2015, [*Online*]. Available: https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

[7] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," presented at the ASIA CCS '11: 6th ACM Symposium on Information, Compuer and Communications Security, Hong Kong China: ACM, Mar. 2011, pp. 355–366. doi: 10.1145/1966913.1966959.

[8] M. Antonakakis *et al.*, "Understanding the Mirai Botnet," in *USENIX Security Symposium*, 2017. [*Online*]. Available: https://api.semanticscholar.org/CorpusID:10552148

[9] O. Al-Jarrah and A. Arafat, "Network Intrusion Detection System using attack behavior classification," presented at the 2014 5th International

Conference on Information and Communication Systems (ICICS), Irbid, Jordan: IEEE, Apr. 2014, pp. 1–6. doi: 10.1109/IACS.2014.6841978.

[10] K. Demertzis, L. Iliadis, and I. Bougoudis, "Gryphon: a semi-supervised anomaly detection system based on one-class evolving spiking neural network," *Neural Comput. Appl.*, vol. 32, no. 9, pp. 4303–4314, May 2020, doi: 10.1007/s00521-019-04363-x.

[11] Y. Zhang, L. Wang, W. Sun, R. C. Green Ii, and M. Alam, "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011, doi: 10.1109/TSG.2011.2159818.

[12] K. N. Junejo and D. Yau, "Data Driven Physical Modelling For Intrusion Detection In Cyber Physical Systems".

[13] Y. Kwon, H. K. Kim, Y. H. Lim, and J. I. Lim, "A behavior-based intrusion detection technique for smart grid infrastructure," in *2015 IEEE Eindhoven PowerTech*, Jun. 2015, pp. 1–6. doi: 10.1109/PTC.2015.7232339.

[14] D. M. Giracca, F. L. Pires, B. Barán, and E. A. M. Jara, "A Deep Learning Approach for Anomaly Detection for Industrial Control Systems," in *2024 L Latin American Computer Conference (CLEI)*, Buenos Aires, Argentina: IEEE, Aug. 2024, pp. 1–10. doi: 10.1109/CLEI64178.2024.10700451.

[15] S. R. B. T. Muda, M. H. M. Yusof, K. M. Alfawaz, M. Balfaqih, and A. Alzahrani, "New Optimized Adaptive Time Series IDS Classifier Algorithm: Beyond Deep Learning," *IEEE Access*, vol. 11, pp. 129882–129904, 2023, doi: 10.1109/ACCESS.2023.3334160.

[16] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System," *IEEE Access*, vol. 8, pp. 83965–83973, 2020, doi: 10.1109/ACCESS.2020.2992249.

[17] S.-W. Lee *et al.*, "Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review," *J. Netw. Comput. Appl.*, vol. 187, p. 103111, Aug. 2021, doi: 10.1016/j.jnca.2021.103111.

[18] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[19] Y. Xue, J. Pan, Y. Geng, Z. Yang, M. Liu, and R. Deng, "Real-Time Intrusion Detection Based on Decision Fusion in Industrial Control Systems," *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 2, pp. 143–153, 2024, doi: 10.1109/TICPS.2024.3406505.

[20] S. Racherla, P. Sripathi, N. Faruqui, M. Alamgir Kabir, M. Whaiduzzaman, and S. Aziz Shah, "Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning," *IEEE Access*, vol. 12, pp. 63584–63597, 2024, doi: 10.1109/ACCESS.2024.3396461.

[21] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997, doi: 10.1162/neco.1997.9.8.1735.

[22] S. Adepu and A. Mathur, "Using Process Invariants to Detect Cyber Attacks on a Water Treatment System," J.-H. Hoepman and S. Katzenbeisser, Eds., Cham: Springer International Publishing, 2016, pp. 91–104. doi: 10.1007/978-3-319-33630-5_7.

[23] F. Apolinário, N. Escravana, É. Hervé, M. L. Pardal, and M. Correia, "FingerCI: generating specifications for critical infrastructures," presented at the SAC '22: The 37th ACM/SIGAPP Symposium on Applied Computing, Virtual Event: ACM, Apr. 2022, pp. 183–186. doi: 10.1145/3477314.3507323.

[24] K. N. Junejo, "Predictive safety assessment for storage tanks of water cyber physical systems using machine learning," *Sādhanā*, vol. 45, no. 1, p. 61, Feb. 2020, doi: 10.1007/s12046-020-1290-y.

[25] S. Seth, G. Singh, and K. Kaur Chahal, "A novel time efficient learning-based approach for smart intrusion detection system," *J. Big Data*, vol. 8, no. 1, p. 111, Dec. 2021, doi: 10.1186/s40537-021-00498-8.

[26] G. Kabasele Ndonda and R. Sadre, "Exploiting the Temporal Behavior of State Transitions for Intrusion Detection in ICS/SCADA," *IEEE Access*, vol. 10, pp. 111171–111187, 2022, doi: 10.1109/ACCESS.2022.3213080.

[27] 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.

[28] A. Sokolov, I. Pyatnitsky, and S. Alabugin, "Applying methods of machine learning in the task of intrusion detection based on the analysis of industrial process state and ICS networking," *FME Trans.*, vol. 47, no. 4, pp. 782–789, 2019, doi: 10.5937/fmet1904782S.

[29] N. L. Ricker, "Decentralized control of the Tennessee Eastman Challenge Process," *J. Process Control*, vol. 6, no. 4, pp. 205–221, 1996, doi: https://doi.org/10.1016/0959-1524(96)00031-5.

[30] P. Zhang, "Industrial control systems," in *Advanced Industrial Control Technology*, Elsevier, 2010, pp. 3–40. doi: 10.1016/B978-1-4377-7807-6.10001-4.

[31] M. Krotofil, "Security of cyber-physical systems: process-aware approach," 2023, doi: 10.15480/882.4913.

[32] S. McLaughlin *et al.*, "The Cybersecurity Landscape in Industrial Control Systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, May 2016, doi: 10.1109/JPROC.2015.2512235.

[33] B. Babu, T. Ijyas, Muneer P., and J. Varghese, "Security issues in SCADA based industrial control systems," in *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, Abha, Saudi Arabia: IEEE, Mar. 2017, pp. 47–51. doi: 10.1109/Anti-Cybercrime.2017.7905261.

[34] E. Hayden, M. Assante, and T. Conway, "An abbreviated history of automation & industrial controls systems and cybersecurity." 2014. [Daring]. Available: https://ics.sans.org/media/An-AbbreviatedHistory-of-Automation-and-ICSCybersecurity.pdf

[35] Kaspersky, "Q3 2024: A Brief Overview of the Main Incidents in Industrial Cybersecurity." [Daring]. Available: https://ics-cert.kaspersky.com/publications/reports/2025/02/19/q3-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/

[36] IBM, "Spear Phishing." [Daring]. Available: https://www.ibm.com/think/topics/spear-phishing

[37] ESET, "New wave of attacks against Ukrainian power industry," *We Live Secur.*, 2016, [Daring]. Available: https://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/

[38] M. Azzam, L. Pasquale, G. Provan, and B. Nuseibeh, "Grounds for Suspicion: Physics-based Early Warnings for Stealthy Attacks on Industrial Control Systems," 2021, *arXiv*. doi: 10.48550/ARXIV.2106.07980.

[39] J. J. Downs and E. F. Vogel, "A plant-wide industrial process control problem," *Comput. Chem. Eng.*, vol. 17, no. 3, pp. 245–255, Mar. 1993, doi: 10.1016/0098-1354(93)80018-I.

[40] Y. Hu, A. Yang, H. Li, Y. Sun, and L. Sun, "A survey of intrusion detection on industrial control systems," *Int. J. Distrib. Sens. Netw.*, vol. 14, no. 8, p. 155014771879461, Aug. 2018, doi: 10.1177/1550147718794615.

[41] R. Mitchell and I.-R. Chen, "Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems," *IEEE Trans.*

Dependable Secure Comput., vol. 12, no. 1, pp. 16–30, Jan. 2015, doi: 10.1109/TDSC.2014.2312327.

[42] M. A. Umer, K. N. Junejo, M. T. Jilani, and A. P. Mathur, "Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations," *Int. J. Crit. Infrastruct. Prot.*, vol. 38, p. 100516, Sep. 2022, doi: 10.1016/j.ijcip.2022.100516.

[43] R. C. Borges Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *2014 7th International Symposium on Resilient Control Systems (ISRCS)*, Aug. 2014, pp. 1–8. doi: 10.1109/ISRCS.2014.6900095.

[44] C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning," *Electron. Mark.*, vol. 31, no. 3, pp. 685–695, Sep. 2021, doi: 10.1007/s12525-021-00475-2.

[45] J. Y. Ryu, H. Y. Chung, and K. Y. Choi, "Potential role of artificial intelligence in craniofacial surgery," *Arch. Craniofacial Surg.*, vol. 22, no. 5, pp. 223–231, Oct. 2021, doi: 10.7181/acfs.2021.00507.

[46] R. Gawde, "Image Caption Generation Methodologies," Apr. 2021.

[47] L. Boué, "Deep learning for pedestrians: backpropagation in CNNs," 2018, *arXiv*. doi: 10.48550/ARXIV.1811.11987.

[48] B. Ding, H. Qian, and J. Zhou, "Activation functions and their characteristics in deep neural networks," in *2018 Chinese Control And Decision Conference (CCDC)*, Shenyang: IEEE, Jun. 2018, pp. 1836–1841. doi: 10.1109/CCDC.2018.8407425.

[49] K. Loaiza, "Deep learning for decision support in dermatology," 2020, doi: 10.13140/RG.2.2.14692.60800.

[50] A. Kagalkar and S. Raghuram, "CORDIC Based Implementation of the Softmax Activation Function," in *2020 24th International Symposium on VLSI Design and Test (VDAT)*, Bhubaneswar, India: IEEE, Jul. 2020, pp. 1–4. doi: 10.1109/VDAT50263.2020.9190498.

[51] S. Yan, "Understanding LSTM and its diagrams," *ML Rev.*, 2016, [Daring]. Available: https://blog.mlreview.com/understanding-lstm-and-its-diagrams-37e2f46f1714

[52] P. Tirchas, D. Drikakis, I. W. Kokkinakis, and S. M. Spottswood, "The effects of hyperparameters on deep learning of turbulent signals," *Phys. Fluids*, vol. 36, no. 12, p. 125174, Dec. 2024, doi: 10.1063/5.0245473.

[53] A. Mao, M. Mohri, and Y. Zhong, "Cross-Entropy Loss Functions: Theoretical Analysis and Applications," 2023. doi: 10.48550/ARXIV.2304.07288.

[54] N. L. Ricker, "Tennessee Eastman Challenge Archive." pp. 38, 40, 2013. [Daring]. Available: http://depts.washington.edu/control/LARRY/TE/download.html

[55] T. Larsson, K. Hestetun, E. Hovland, and S. Skogestad, "Self-Optimizing Control of a Large-Scale Plant: The Tennessee Eastman Process," *Ind. Eng. Chem. Res.*, vol. 40, no. 22, pp. 4889–4901, Oct. 2001, doi: 10.1021/ie000586y.

[56] N. L. Ricker, "Optimal steady-state operation of the Tennessee Eastman challenge process," *Comput. Chem. Eng.*, vol. 19, no. 9, pp. 949–959, Sep. 1995, doi: 10.1016/0098-1354(94)00043-N.

[57] N. L. Ricker and J. H. Lee, "Ndaringar modeling and state estimation for the Tennessee Eastman challenge process," *Comput. Chem. Eng.*, vol. 19, no. 9, pp. 983–1005, Sep. 1995, doi: 10.1016/0098-1354(94)00113-3.