DAFTAR PUSTAKA

Ajmal, A. B., Alam, M., Khaliq, A. A., Khan, S., Qadir, Z., & Mahmud, M. A. P. (2021). Last Line of Defense: Reliability through Inducing Cyber Threat Hunting with Deception in SCADA Networks. *IEEE Access*, *9*, 126789–126800. https://doi.org/10.1109/ACCESS.2021.3111420

Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access*, *8*, 83965–83973. https://doi.org/10.1109/ACCESS.2020.2992249

Al-safaar, D. (2023). *Hybrid AE-MLP : Hybrid Deep Learning Model Based on Autoencoder and Multilayer Perceptron Model for Intrusion Detection System*. *16*(2). https://doi.org/10.22266/ijies2023.0430.04

Amien, J. Al, Ghani, H. A., Saleh, N. I., Ismanto, E., & Gunawan, R. (2023). *Intrusion detection system for imbalance ratio class using weighted XGBoost classifier*. *21*(5), 1102–1112. https://doi.org/10.12928/TELKOMNIKA.v21i5.24735

Amru, M., Kannan, R. J., & Ganesh, E. N. (2024). *Network intrusion detection system by applying ensemble model for smart home*. *14*(3), 3485–3494. https://doi.org/10.11591/ijece.v14i3.pp3485-3494

Anton, S. D., Kanoor, S., Fraunholz, D., & Schotten, H. D. (2018). Evaluation of machine learning-based anomaly detection algorithms on an industrial modbus/TCP data set. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3230833.3232818

Arifin, M. A. S., Stiawan, D., Susanto, Rejito, J., Idris, M. Y., & Budiarto, R. (2021). Denial of Service Attacks Detection on SCADA Network IEC 60870-5-104 using Machine Learning. *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, *2021-Octob*(October), 228–232. https://doi.org/10.23919/EECSI53397.2021.9624255

Asiri, M., Arunasalam, A., Saxena, N., & Celik, Z. B. (2025). Frontline responders: Rethinking indicators of compromise for industrial control system security. *Computers and Security*, *154*(March). https://doi.org/10.1016/j.cose.2025.104421

Balla, A., Habaebi, M. H., Elsheikh, E. A. A., Islam, M. R., & Suliman, F. M. (2023). The Effect of Dataset Imbalance on the Performance of SCADA Intrusion Detection Systems. *Sensors*, *23*(2). https://doi.org/10.3390/s23020758

Barbieri, G., Conti, M., Tippenhauer, N. O., & Turrin, F. (2021). Assessing the Use of Insecure ICS Protocols via IXP Network Traffic Analysis. *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, *2021-July*. https://doi.org/10.1109/ICCCN52240.2021.9522219

Bashendy, M., Eltanbouly, S., Tantawy, A., & Erradi, A. (2021). *Design and Implementation of Cyber-Physical Attacks on Modbus/TCP Protocol*. *December*,

38–45. https://doi.org/10.20533/wcicss.2020.0005

Bristow, M. (2021). *A SANS 2021 Survey: OT/ICS Cybersecurity*. *August*, 1–23. www.cisa.gov/critical-infrastructure-sectors

Broad, W. J., Markoff, J., & Sanger, D. E. (n.d.). *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*. Retrieved February 19, 2024, from https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Cerf, E. (2024). *Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world*. https://news.ucsc.edu/2024/05/ukraine-cybersecurity/

Chen, J., Lalor, J., Liu, W., Druhl, E., Granillo, E., Vimalananda, V. G., & Yu, H. (2019). Detecting Hypoglycemia Incidents Reported in Patients' Secure Messages: Using Cost-Sensitive Learning and Oversampling to Reduce Data Imbalance. *Journal of Medical Internet Research*, *21*(3). https://doi.org/10.2196/11990

Cichonski, P. (2025). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. In *NIST Special Publication* (Vols. 800–61). http://dx.doi.org/10.6028/NIST.SP.800-61r2%5Cnhttp://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Conti, M., Donadel, D., & Turrin, F. (2021). A Survey on Industrial Control System Testbeds and Datasets for Security Research. *IEEE Communications Surveys and Tutorials*, *23*(4), 2248–2294. https://doi.org/10.1109/COMST.2021.3094360

Eaton, C., & Volz, D. (2021). *U.S. Pipeline cyberattack forces closure*. https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

Eltayeb, R. Y., Karrar, A. E., Osman, W. I., & Mutasim, M. (2023). Handling Imbalanced Data through Re-sampling: Systematic Review. *Indonesian Journal of Electrical Engineering and Informatics*, *11*(2), 503–514. https://doi.org/10.52549/ijeei.v11i2.4471

Farhana, K., Rahman, M., & Ahmed, T. (2020). *An intrusion detection system for packet and flow based networks using deep neural network approach*. *10*(5), 5514–5525. https://doi.org/10.11591/ijece.v10i5.pp5514-5525

Filkins, B., & Wylie, D. (2019). *Information Security Reading Room SANS 2019 State of OT / ICS Cybersecurity Survey*, *SANS 2019 State of OT / ICS Cybersecurity Survey Written by Barbara Filkins*.

Gao, X., Shan, C., Hu, C., Niu, Z., & Liu, Z. (2019). An Adaptive Ensemble Machine Learning Model for Intrusion Detection. *IEEE Access*, *7*, 82512–82521. https://doi.org/10.1109/ACCESS.2019.2923640

Gill, N. S., & Gulia, P. (2025). *A review on machine learning based intrusion detection system for internet of things enabled environment*. *14*(2), 1890–1898. https://doi.org/10.11591/ijece.v14i2.pp1890-1898

Gómez, Á. L. P., Maimó, L. F., Celdrán, A. H., Clemente, F. lix J. G. a., Sarmiento, C. C., Masa, C. J. D. C., & Nistal, R. n. M. nde. (2019). On the Generation of Anomaly Detection Datasets in Industrial Control Systems. *IEEE Access*, *7*, 177460–177473. https://doi.org/10.1109/ACCESS.2019.2958284

Harwahyu, R., Henri, F., Ndolu, E., & Overbeek, M. V. (2024). *Three layer hybrid learning to improve intrusion detection system performance*. *14*(2), 1691–1699. https://doi.org/10.11591/ijece.v14i2.pp1691-1699

Idrissi, I., Boukabous, M., Azizi, M., Moussaoui, O., & Fadili, H. El. (2021). *Toward a deep learning-based intrusion detection system for IoT against botnet attacks*. *10*(1), 110–120. https://doi.org/10.11591/ijai.v10.i1.pp110-120

Jahromi, A. N., Karimipour, H., Dehghantanha, A., & Choo, K. K. R. (2021). Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber-Physical Systems. *IEEE Internet of Things Journal*, *8*(17), 13712–13722. https://doi.org/10.1109/JIOT.2021.3067667

Jaradat, A. S., Barhoush, M. M., & Easa, R. B. (2022). *Network intrusion detection system : machine learning approach*. *25*(2), 1151–1158. https://doi.org/10.11591/ijeecs.v25.i2.pp1151-1158

Jiang, J. R., & Chen, Y. T. (2022). Industrial Control System Anomaly Detection and Classification Based on Network Traffic. *IEEE Access*, *10*, 41874–41888. https://doi.org/10.1109/ACCESS.2022.3167814

Joloudari, J. H., Marefat, A., Nematollahi, M. A., Oyelere, S. S., & Hussain, S. (2023). Effective Class-Imbalance Learning Based on SMOTE and Convolutional Neural Networks. *Applied Sciences (Switzerland)*, *13*(6). https://doi.org/10.3390/app13064006

Kante, M., Sharma, V., & Gupta, K. (2024). Mitigating ransomware attacks through cyber threat intelligence and machine learning. *Indonesian Journal of Electrical Engineering and Computer Science*, *33*(3), 1958–1965. https://doi.org/10.11591/ijeecs.v33.i3.pp1958-1965

Krotofil, M., Kursawe, K., & Gollmann, D. (2019). Securing industrial control systems. *Advanced Sciences and Technologies for Security Applications*, *June*, 3–27. https://doi.org/10.1007/978-3-030-12330-7_1

Lin, C. C., Deng, D. J., Kuo, C. H., & Chen, L. (2019). Concept drift detection and adaption in big imbalance industrial IoT data using an ensemble learning method of offline classifiers. *IEEE Access*, *7*, 56198–56207. https://doi.org/10.1109/ACCESS.2019.2912631

Lopez, A. D. (2019). Network Traffic Behavioral Analytics for Detection of DDoS Attacks. *SMU Data Science Review*, *2*(1), 25.

Louk, M. H. L., & Tama, B. A. (2021). Exploring ensemble-based class imbalance learners for intrusion detection in industrial control networks. *Big Data and Cognitive Computing*, *5*(4). https://doi.org/10.3390/bdcc5040072

Lusito, S., Pugnana, A., & Guidotti, R. (2023). Solving imbalanced learning with outlier detection and features reduction. *Machine Learning*, *0123456789*. https://doi.org/10.1007/s10994-023-06448-0

Magdy, M. E., Matter, A. M., Hussin, S., Hassan, D., & Elsaid, S. A. (2023). *Anomaly-based intrusion detection system based on feature selection and majority voting*. *30*(3), 1699–1706. https://doi.org/10.11591/ijeecs.v30.i3.pp1699-1706

Manikandan, D., & Dhilipan, J. (2024). Machine learning approach for intrusion detection system using dimensionality reduction. *Indonesian Journal of Electrical Engineering and Computer Science*, *34*(1), 430–440. https://doi.org/10.11591/ijeecs.v34.i1.pp430-440

Mghames, S. A. Z., & Ibrahim, A. A. (2023). *Intrusion detection system for detecting distributed denial of service attacks using machine learning algorithms*. *32*(1), 304–311. https://doi.org/10.11591/ijeecs.v32.i1.pp304-311

Modbus, S. (n.d.). *No Title*. Retrieved November 28, 2022, from https://www.simplymodbus.ca/TCP.htm

Ning, B., Qiu, S., Zhao, T., & Li, Y. (2020). *Power IoT Attack Samples Generation and Detection Using Generative Adversarial Networks*. 3721–3724. https://doi.org/10.1109/EI250167.2020.9346661

Pinto, A. Di, Dragoni, Y., & Carcano, A. (2018). TRITON: The first ICS cyber attack on safety instrument systems. *Black Hat USA*, 1–26.

Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *IEEE Communications Surveys and Tutorials*, *22*(3), 1942–1976. https://doi.org/10.1109/COMST.2020.2987688

Prabu, K., & Sudhakar, P. (2024). A hybrid deep learning approach for enhanced network intrusion detection. *Indonesian Journal of Electrical Engineering and Computer Science*, *33*(3), 1915–1923. https://doi.org/10.11591/ijeecs.v33.i3.pp1915-1923

Rahman, A., Mustafa, G., Khan, A. Q., Abid, M., & Durad, M. H. (2022). Launch of denial of service attacks on the modbus/TCP protocol and development of its protection mechanisms. *International Journal of Critical Infrastructure Protection*, *39*(September), 100568. https://doi.org/10.1016/j.ijcip.2022.100568

Raihan-Al-Masud, M., & Mustafa, H. A. (2019). Network Intrusion Detection System Using Voting Ensemble Machine Learning. *3rd IEEE International Conference on Telecommunications and Photonics, ICTP 2019*, 8–11. https://doi.org/10.1109/ICTP48844.2019.9041736

Rajesh, L., & Satyanarayana, P. (2022). Evaluation of Machine Learning Algorithms for Detection of Malicious Traffic in SCADA Network. *Journal of Electrical Engineering and Technology*, *17*(2), 913–928. https://doi.org/10.1007/s42835-021-00931-1

Rakas, S. V. B., Stojanovic, M. D., & Markovic-Petrovic, J. D. (2020). A review of research work on network-based SCADA intrusion detection systems. *IEEE Access*, *8*, 93083–93108. https://doi.org/10.1109/ACCESS.2020.2994961

Ranade, V. (2021). *A laboratory for cyber-attack generation and testing in Indus trial Control Systems: Design and Simulation*.

https://resolver.tudelft.nl/uuid:ad554d68-4503-4544-b51b-e48379fc7216

Riyadh, M., & Alshibani, D. R. (2021). *Intrusion detection system based on machine learning techniques*. *23*(2), 953–961. https://doi.org/10.11591/ijeecs.v23.i2.pp953-961

Rodofile, N. R. (2013). *Generating Attacks and Labelling Attack Datasets for Industrial Control Intrusion Detection Systems*.

Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. *International Journal of Critical Infrastructure Protection*, *25*, 14–35. https://doi.org/10.1016/j.ijcip.2019.01.002

Rolansa, F., Istiyanto, J. E., Afiahayati, A., & Frisky, A. Z. K. (2025). *SMOTE tree-based autoencoder multi-stage detection for man- in-the-middle in SCADA*. *38*(1), 133–144. https://doi.org/10.11591/ijeecs.v38.i1.pp133-144

Saed, M., & Aljuhani, A. (2022). Detection of Man in the Middle Attack using Machine learning. *Proceedings of 2022 2nd International Conference on Computing and Information Technology, ICCIT 2022*, 388–393. https://doi.org/10.1109/ICCIT52419.2022.9711555

SICARD, F., ZAMAI, É., & FLAUS, J. M. (2019). An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems. *Reliability Engineering and System Safety*, *188*(March 2018), 584–603. https://doi.org/10.1016/j.ress.2019.03.020

Talukder, M. A., Sharmin, S., Uddin, M. A., Islam, M. M., & Aryal, S. (2024). MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs. *International Journal of Information Security*, *23*(3), 2139–2158. https://doi.org/10.1007/s10207-024-00833-z

Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2022). Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. *International Journal of Critical Infrastructure Protection*, *38*. https://doi.org/10.1016/j.ijcip.2022.100516

Vadhil, F. A., Salihi, M. L., & Nanne, M. F. (2024). *Machine learning-based intrusion detection system for detecting web attacks*. *13*(1), 711–721. https://doi.org/10.11591/ijai.v13.i1.pp711-721

Waagsnes, H., & Ulltveit-Moe, N. (2018). Intrusion detection system test framework for SCADA systems. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *2018-Janua*(Icissp), 275–285. https://doi.org/10.5220/0006588202750285

Wan, M., Shang, W., & Zeng, P. (2017). Double Behavior Characteristics for One-Class Classification Anomaly Detection in Networked Control Systems. *IEEE Transactions on Information Forensics and Security*, *12*(12), 3011–3023. https://doi.org/10.1109/TIFS.2017.2730581

Wang, N., Chen, Y., Hu, Y., Lou, W., & Hou, Y. T. (2021). MANDA: On adversarial example detection for network intrusion detection system. *Proceedings - IEEE INFOCOM*, *2021-May*, 1–10. https://doi.org/10.1109/INFOCOM42981.2021.9488874

Wlazlo, P., Sahu, A., Mao, Z., Huang, H., Goulart, A., Davis, K., & Zonouz, S. (2021). Man-in-the-middle attacks and defence in a power system cyber-physical testbed. In *IET Cyber-Physical Systems: Theory and Applications* (Vol. 6, Issue 3, pp. 164–177). https://doi.org/10.1049/cps2.12014

Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*, *34*, 100433. https://doi.org/10.1016/j.ijcip.2021.100433

Yang, H., Cheng, L., & Chuah, M. C. (2019). Deep-Learning-Based Network Intrusion Detection for SCADA Systems. *2019 IEEE Conference on Communications and Network Security, CNS 2019*. https://doi.org/10.1109/CNS.2019.8802785

Yuan, Y., Wei, J., Huang, H., Jiao, W., Wang, J., & Chen, H. (2023). Review of resampling techniques for the treatment of imbalanced industrial data classification in equipment condition monitoring. *Engineering Applications of Artificial Intelligence*, *126*(PB), 106911. https://doi.org/10.1016/j.engappai.2023.106911