

## DAFTAR PUSTAKA

- [1] X. Liu, T. Shi, C. Xie, and D. Song, “UniFed: A Benchmark for Federated Learning Frameworks,” *ResearchGate*, Jul. 21, 2022. [https://www.researchgate.net/publication/362172252\\_UniFed\\_A\\_Benchmark\\_for\\_Federated\\_Learning\\_Frameworks](https://www.researchgate.net/publication/362172252_UniFed_A_Benchmark_for_Federated_Learning_Frameworks) (accessed Jan. 10, 2024).
- [2] L. Lavaur, M.-O. Pahl, Yann Busnel, and Fabien Autrel, “The Evolution of Federated Learning-Based Intrusion Detection and Mitigation: A Survey,” *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2309–2332, Sep. 2022, doi: <https://doi.org/10.1109/tnsm.2022.3177512>.
- [3] “Coordinated Attacks Against Federated Learning: A Multi-Agent Reinforcement Learning Approach,” *Iclr.cc*, 2024. <https://iclr.cc/virtual/2021/4199> (accessed Jan. 10, 2024).
- [4] M. Sarhan, Siamak Layeghy, N. Moustafa, and M. Portmann, “Cyber Threat Intelligence Sharing Scheme Based on Federated Learning for Network Intrusion Detection,” *Journal of Network and Systems Management*, vol. 31, no. 1, Oct. 2022, doi: <https://doi.org/10.1007/s10922-022-09691-3>.
- [5] Y.-S. Wu, B. Foo, Y. Mei, and S. Bagchi, “Collaborative intrusion detection system (CIDS): framework for accurate and efficient IDS,” Jul. 2004, doi: <https://doi.org/10.1109/csac.2003.1254328>.
- [6] Mashal Khana., Frank G. Glavina., Matthias Nicklesa., (2023). Federated Learning as a Privacy Solution – An Overview. Published by Elsevier B.V
- [7] Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Bhattacharya, S., Maddikunta, P. K., & Gadekallu, T. R. (2021). Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions. *ArXiv*. /abs/2106.09527
- [8] Arif Yulianto., Parman Sukarno” and Novian Anggis Suwastika (2019). Improving AdaBoost-based Intrusion Detection System (IDS) Performance on CIC IDS 2017 Dataset. *Journal of Physics Conference Series* 1192:012018. DOI: 10.1088/1742-6596/1192/1/012018
- [9] Rodríguez, M.; Alesanco, Á.; Mehavilla, L.; García, J. Evaluation of Machine Learning Techniques for Traffic Flow-Based Intrusion Detection. *Sensors* 2022, 22, 9326. <https://doi.org/10.3390/s22239326>
- [10] Bayu, I. M. K., Prasasti, A. L., & Maryopi, D. (2022). Analisis Performa Federated Learning Untuk Klasifikasi Gambar Yang Sensitif Terhadap Privasi Data. *eProceedings of Engineering*, 9(3).
- [11] Kyuho Jason Lee, “Architecture of neural processing unit for deep neural networks,” *Advances in Computers*, pp. 217–245, Jan. 2021, doi: <https://doi.org/10.1016/bs.adcom.2020.11.001>.
- [12] Zhou, C. V., Leckie, C., & Karunasekera, S. (2010). A survey of coordinated attacks and collaborative intrusion detection. *Computers & Security*, 29(1), 124-140. <https://doi.org/10.1016/j.cose.2009.06.008>

- [13] Y. Huang, Z. Xiong, and Q. Zhu, "Cross-Layer Coordinated Attacks on Cyber-Physical Systems: A LQG Game Framework with Controlled Observations," *2021 European Control Conference (ECC)*, Jun. 2021, doi: <https://doi.org/10.23919/ecc54610.2021.9654874>.
- [14] ] Azhari Shouni Barkah., Siti Rahayu Selamat., Zaheera Zainal Abidin., Rizki Wahyudi1. (2023). Data Generative Model to Detect the Anomalies for IDS Imbalance CICIDS2017 Dataset. *TEM Journal*. Volume 12, Issue 1, pages 80-89, ISSN 2217-8309, DOI: 10.18421/TEM121-11, February 2023.
- [15] Shailesh Singh Panwar, Pritam Singh Negi, Lokesh Singh Panwar, Y. P. Raiwani. (2019). Implementation of Machine Learning Algorithms on CICIDS-2017 Dataset for Intrusion Detection Using WEKA. *International Journal of Recent Technology and Engineering (IJRTE)* ISSN: 2277-3878, Volume-8, Issue-3, September 2019
- [16] Alrowaily, M., Alenezi, F., Lu, Z. (2019). Effectiveness of Machine Learning Based Intrusion Detection Systems. In: Wang, G., Feng, J., Bhuiyan, M., Lu, R. (eds) *Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2019. Lecture Notes in Computer Science()*, vol 11611. Springer, Cham. [https://doi.org/10.1007/978-3-030-24907-6\\_21](https://doi.org/10.1007/978-3-030-24907-6_21)
- [17] N. Bindra and M. Sood, "Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset," *Autom. Control Comput. Sci.*, vol. 53, no. 5, pp. 419–428, Sep. 2019
- [18] Rao YN, Suresh Babu K. An Imbalanced Generative Adversarial Network-Based Approach for Network Intrusion Detection in an Imbalanced Dataset. *Sensors (Basel)*. 2023 Jan 3;23(1):550. doi: 10.3390/s23010550. PMID: 36617148; PMCID: PMC9824750.
- [19] G. Karatas, O. Demir and O. Koray Sahingoz, "Deep Learning in Intrusion Detection Systems," 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 2018, pp. 113-116, doi: 10.1109/IBIGDELFT.2018.8625278.
- [20] Y. Fu, Y. Du, Z. Cao, and W. Xiang, "A Deep Learning Model for Network Intrusion Detection with Imbalanced Data," *ResearchGate*, Mar. 14, 2022. [https://www.researchgate.net/publication/359232449\\_A\\_Deep\\_Learning\\_Model\\_for\\_Network\\_Intrusion\\_Detection\\_with\\_Imbalanced\\_Data](https://www.researchgate.net/publication/359232449_A_Deep_Learning_Model_for_Network_Intrusion_Detection_with_Imbalanced_Data) (accessed Jan. 10, 2024).
- [21] T. Sun, D. Li, and B. Wang, "Decentralized Federated Averaging," *ResearchGate*, Apr.22,2021.[https://www.researchgate.net/publication/351095575\\_Decentralized\\_Federated\\_Averaging](https://www.researchgate.net/publication/351095575_Decentralized_Federated_Averaging) (accessed Jan. 10, 2024).
- [22] V. K. Navya, J. Adithi, D. Rudrawal, H. Tailor and N. James, "Intrusion Detection System using Deep Neural Networks (DNN)," 2021 International Conference on Advancements in Electrical, Electronics, Communication, *Computing and Automation (ICAECA)*, Coimbatore, India, 2021, pp. 1-6, doi: 10.1109/ICAECA52838.2021.9675513. <https://ieeexplore.ieee.org/document/9675513>
- [23] J. Jose and D. V. Jose, "Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset," *ResearchGate*, Feb. 2023.

[https://www.researchgate.net/publication/367762160\\_Deep\\_learning\\_algorithms\\_for\\_intrusion\\_detection\\_systems\\_in\\_internet\\_of\\_things\\_using\\_CIC-IDS\\_2017\\_dataset](https://www.researchgate.net/publication/367762160_Deep_learning_algorithms_for_intrusion_detection_systems_in_internet_of_things_using_CIC-IDS_2017_dataset) (accessed Jan. 10, 2024).

[24] Jayant Gadge and A. Patil, "Port scan detection," Jan. 2008, doi: <https://doi.org/10.1109/icon.2008.4772622>.

[25] M. S. Koli and M. K. Chavan, "An advanced method for detection of botnet traffic using intrusion detection system," Mar. 2017, doi: <https://doi.org/10.1109/iciict.2017.7975246>.

[26] M. Abadi, P. Barham, J. Chen, and X. Zhang, "TensorFlow: A system for large-scale machine learning," *ResearchGate*, May 27, 2016. [https://www.researchgate.net/publication/303657108\\_TensorFlow\\_A\\_system\\_for\\_large-scale\\_machine\\_learning](https://www.researchgate.net/publication/303657108_TensorFlow_A_system_for_large-scale_machine_learning) (accessed Jan. 23, 2024).