

REFERENCES

- [1] G. Aceto, V. Persico, and A. Pescapé, “Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0,” *Journal of Industrial Information Integration*, vol. 18, p. 100129, 2020, doi: 10.1016/j.jii.2020.100129.
- [2] P. Rani and R. Sharma, “Intelligent transportation system for internet of vehicles based vehicular networks for smart cities,” *Computers and Electrical Engineering*, vol. 105, 2023, doi: 10.1016/j.compeleceng.2022.108543.
- [3] P. K. Malik, R. Singh, A. Gehlot, S. V. Akram, and P. K. Das, “Village 4.0: Digitalization of village with smart internet of things technologies,” *Computers and Industrial Engineering*, vol. 165, p. 107938, 2022, doi: 10.1016/j.cie.2022.107938.
- [4] A. Djenna, S. Harous, and D. E. Saidouni, “Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure,” *Applied Sciences (Switzerland)*, vol. 11, 2021, doi: 10.3390/app11104580.
- [5] W. Li, W. Meng, and L. F. Kwok, “Surveying trust-based collaborative intrusion detection: State-of-the-art, challenges and future directions,” *IEEE Communications Surveys and Tutorials*, vol. 24, pp. 280–305, 2022, doi: 10.1109/COMST.2021.3139052.
- [6] K. H. Li, P. P. B. de Gusmão, D. J. Beutel, and N. D. Lane, “Secure aggregation for federated learning in flower,” in *Proceedings of the 2nd ACM International Workshop on Distributed Machine Learning*, ser. DistributedML ’21. Association for Computing Machinery, 2021, p. 8–14, doi: 10.1145/3488659.3493776.
- [7] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, vol. 54. PMLR, 2017, pp. 1273–1282.
- [8] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, “Federated optimization in heterogeneous networks,” in *Proceedings of Machine Learning and Systems*, vol. 2, 2020, pp. 429–450.

- [9] P. Dahiya and S. Bhattacharya, "Miraibotguard: Federated learning for intelligent defense against mirai threats," in *Proceedings - 2nd IEEE International Conference on Device Intelligence, Computing and Communication Technologies, DICCT 2024*. Institute of Electrical and Electronics Engineers Inc., 2024, pp. 358–363, doi: 10.1109/DICCT61038.2024.10533028.
- [10] S. Prasad, I. Sharma, and D. Rajendraprasad, "Federated learning models for intrusion detection in industrial iot networks," in *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*. IEEE, 2024, pp. 1260–1265, doi: 10.1109/ICCPCT61902.2024.10672938.
- [11] Y. Chen, F. Fang, B. Wang, and L. Zhang, "An efficient federated learning framework for iot intrusion detection," in *IEEE Vehicular Technology Conference*. Institute of Electrical and Electronics Engineers Inc., 2024, doi: 10.1109/VTC2024-Fall63153.2024.10757488.
- [12] A. Rejeb, K. Rejeb, S. Simske, H. Treiblmaier, and S. Zailani, "The big picture on the internet of things and the smart city: a review of what we know and what we need to know," *Internet of Things*, vol. 19, p. 100565, 2022, doi: 10.1016/j.iot.2022.100565.
- [13] M. J. Mahdi, A. F. Aljuboori, and M. H. Ali, "Smart stadium using cloud computing and internet of things (iot): Existing and new models," *International Journal of Computer Applications Technology and Research*, vol. 10, pp. 111–118, 2021, doi: 10.7753/ijcatr1005.1002.
- [14] T. Mazhar, D. B. Talpur, T. A. Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, K. Ouahada, and H. Hamam, "Analysis of iot security challenges and its solutions using artificial intelligence," *Brain Sciences*, vol. 13, 2023, doi: 10.3390/brain-sci13040683.
- [15] A. EFE and İrem Nur ABACI, "Comparison of the host based intrusion detection systems and network based intrusion detection systems," *Celal Bayar Üniversitesi Fen Bilimleri Dergisi*, vol. 18, pp. 23–32, 2022, doi: 10.18466/cbayarfbe.832533.
- [16] Y. Otoum and A. Nayak, "As-ids: Anomaly and signature based ids for the internet of things," *Journal of Network and Systems Management*, vol. 29, 2021, doi: 10.1007/s10922-021-09589-6.

- [17] S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, “Internet of things intrusion detection: Centralized, on-device, or federated learning?” *IEEE Network*, vol. 34, pp. 310–317, 2020, doi: 10.1109/MNET.011.2000286.
- [18] L. Li, Y. Fan, M. Tse, and K.-Y. Lin, “A review of applications in federated learning,” *Computers Industrial Engineering*, vol. 149, p. 106854, 2020, doi: 10.1016/j.cie.2020.106854.
- [19] Z. Qin, G. Y. Li, and H. Ye, “Federated learning and wireless communications,” *IEEE Wireless Communications*, vol. 28, no. 5, pp. 134–140, 2021, doi: 10.1109/MWC.011.2000501.
- [20] Z. Zhao, C. Feng, W. Hong, J. Jiang, C. Jia, T. Q. S. Quek, and M. Peng, “Federated learning with non-iid data in wireless networks,” *IEEE Transactions on Wireless Communications*, vol. 21, no. 3, pp. 1927–1942, 2022, doi: 10.1109/TWC.2021.3108197.
- [21] J. A. de Oliveira, V. P. Gonçalves, R. I. Meneguette, R. T. de Sousa, D. L. Guidoni, J. C. Oliveira, and G. P. Rocha Filho, “F-nids — a network intrusion detection system based on federated learning,” *Computer Networks*, vol. 236, p. 110010, 2023, doi: 10.1016/j.comnet.2023.110010.
- [22] W. Samek, G. Montavon, S. Lapuschkin, C. J. Anders, and K. R. Müller, “Explaining deep neural networks and beyond: A review of methods and applications,” *Proceedings of the IEEE*, vol. 109, pp. 247–278, 2021, doi: 10.1109/JPROC.2021.3060483.
- [23] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, “Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment,” *Sensors*, vol. 23, 2023, doi: 10.3390/s23135941.
- [24] L. Cao, “Beyond i.i.d.: Non-iid thinking, informatics, and learning,” *IEEE Intelligent Systems*, vol. 37, no. 4, pp. 5–17, 2022, doi: 10.1109/MIS.2022.3194618.
- [25] T. Chen and C. Guestrin, “Xgboost: A scalable tree boosting system,” in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, vol. 13. Association for Computing Machinery, 2016, pp. 785–794, doi: 10.1145/2939672.2939785.

- [26] Z. Zhou, H. Huang, and B. Fang, “Application of weighted cross-entropy loss function in intrusion detection,” *Journal of Computer and Communications*, vol. 09, pp. 1–21, 2021, doi: 10.4236/jcc.2021.911001.
- [27] Željko Vujović, “Classification model evaluation metrics,” *International Journal of Advanced Computer Science and Applications*, vol. 12, pp. 599–606, 2021, doi: 10.14569/IJACSA.2021.0120670.