REFERENCES

[1] K. Elgazzar *et al.*, "Revisiting the internet of things: New trends, opportunities and grand challenges," *Frontiers in the Internet of Things*, vol. 1, Nov. 2022, doi: 10.3389/friot.2022.1073780.

[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE Trans. Industr. Inform.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018, doi: 10.1109/TII.2018.2852491.

[3] L. Diana, P. Dini, and D. Paolini, "Overview on Intrusion Detection Systems for Computers Networking Security," *Computers*, vol. 14, no. 3, p. 87, Mar. 2025, doi: 10.3390/computers14030087.

[4] M. M. Rahman, S. Al Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," *Cyber Security and Applications*, vol. 3, Dec. 2024, doi: 10.1016/j.csa.2024.100082.

[5] A. Thakkar and R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, Jun. 2021, doi: 10.1007/s11831-020-09496-0.

[6] W. Wang, H. Yang, C. Meinel, H. Y. Özkan, C. B. Serna, and C. Mas-Machuca, "Feature Distribution Shift Mitigation with Contrastive Pretraining for Intrusion Detection," in *2024 IEEE International Conference on Machine Learning for Communication and Networking (ICMLCN)*, IEEE, May 2024, pp. 177–182. doi: 10.1109/ICMLCN59089.2024.10624758.

[7] S. Mahadik, P. M. Pawar, and R. Muthalagu, "Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT)," *Journal of Network and Systems Management*, vol. 31, no. 1, p. 2, Jan. 2023, doi: 10.1007/s10922-022-09697-x.

[8] B. A. Alahmadi, L. Axon, and I. Martinovic, "99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms," Boston: USENIX Association, Aug. 2022, pp. 2783–2800. [Online].

Available: https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi

[9] M. A. Bilal, I. Ul Islam, S. Idrees, M. Qasim, M. J. Khan, and J. Khan, "Dataset-centric evaluation of federated intrusion detection models in IoT networks," *Sci. Rep.*, vol. 16, no. 1, p. 2683, Jan. 2026, doi: 10.1038/s41598-025-32567-w.

[10] E. Mushtaq, A. Zameer, and A. Khan, "A two-stage stacked ensemble intrusion detection system using five base classifiers and MLP with optimal feature selection," *Microprocess. Microsyst.*, vol. 94, p. 104660, Oct. 2022, doi: 10.1016/j.micpro.2022.104660.

[11] B. A. Tama and S. Lim, "Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation," Feb. 01, 2021, *Elsevier Ireland Ltd*. doi: 10.1016/j.cosrev.2020.100357.

[12] L. Grinsztajn, E. Oyallon, and G. Varoquaux, "Why do tree-based models still outperform deep learning on typical tabular data?," in *36th Conference on Neural Information Processing Systems (NeurIPS 2022) Track on Datasets and Benchmarks.*,

[13] T. Chen and C. Guestrin, "XGBoost," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, NY, USA: ACM, Aug. 2016, pp. 785–794. doi: 10.1145/2939672.2939785.

[14] G. Ke *et al.*, "LightGBM: A Highly Efficient Gradient Boosting Decision Tree," in *Advances in Neural Information Processing Systems 30 (NeurIPS 2017)*, 2017.

[15] T. G. Dietterich, "Ensemble Methods in Machine Learning," 2000, pp. 1–15. doi: 10.1007/3-540-45014-9_1.

[16] Kai Ming Ting and Ian H. Witten, "Stacking-Bagged-and-Dagged-Models.," in *ICML '97: Proceedings of the Fourteenth International Conference on Machine Learning*,

[17] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and Adna N Anwar, "TON-IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-

driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020, doi: 10.1109/ACCESS.2020.3022862.

[18] J. Pineau *et al.*, "Improving Reproducibility in Machine Learning Research (A Report from the NeurIPS 2019 Reproducibility Program)," *Journal of Machine Learning Research*, vol. 22, pp. 1–20, May 2021.

[19] S. Ismail, S. Dandan, and A. Qushou, "Intrusion Detection in IoT and IIoT: Comparing Lightweight Machine Learning Techniques Using TON_IoT, WUSTL-IIOT-2021, and EdgeIIoTset Datasets," *IEEE Access*, vol. 13, pp. 73468–73485, 2025, doi: 10.1109/ACCESS.2025.3554083.

[20] M. Masum *et al.*, "Bayesian Hyperparameter Optimization for Deep Neural Network-Based Network Intrusion Detection," in *2021 IEEE International Conference on Big Data (Big Data)*, IEEE, Dec. 2021, pp. 5413–5419. doi: 10.1109/BigData52589.2021.9671576.

[21] S. Jamshidi, K. W. Nafi, A. Nikanjam, and F. Khomh, "Evaluating machine learning-driven intrusion detection systems in IoT: Performance and energy consumption," *Comput. Ind. Eng.*, vol. 204, p. 111103, Jun. 2025, doi: 10.1016/j.cie.2025.111103.

[22] University of New South Wales (UNSW), "The TON_IoT Datasets." Accessed: Nov. 25, 2025. [Online]. Available: https://research.unsw.edu.au/projects/toniot-datasets

[23] T. Saito and M. Rehmsmeier, "The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets," *PLoS One*, vol. 10, no. 3, Mar. 2015, doi: 10.1371/journal.pone.0118432.

[24] D. Kus *et al.*, "A False Sense of Security?," in *Proceedings of the 8th ACM on Cyber-Physical System Security Workshop*, New York, NY, USA: ACM, May 2022, pp. 73–84. doi: 10.1145/3494107.3522773.

[25] M. Mia, M. M. A. Pritom, T. Islam, and K. Hasan, "Visually Analyze SHAP Plots to Diagnose Misclassifications in ML-based Intrusion Detection," Nov. 2024, [Online]. Available: http://arxiv.org/abs/2411.02670

[26] A. Pinto, L. C. Herrera, Y. Donoso, and J. A. Gutierrez, "Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the

Protection of Critical Infrastructure," Mar. 01, 2023, *MDPI*. doi: 10.3390/s23052415.

[27] D. L. Marino, C. S. Wickramasinghe, and M. Manic, "An Adversarial Approach for Explainable AI in Intrusion Detection Systems," Nov. 2018, [Online]. Available: http://arxiv.org/abs/1811.11705

[28] L. Breiman, "Random Forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, Oct. 2001, doi: 10.1023/A:1010933404324.

[29] C. Molnar, G. Casalicchio, and B. Bischl, "Interpretable Machine Learning – A Brief History, State-of-the-Art and Challenges," 2020, pp. 417–431. doi: 10.1007/978-3-030-65965-3_28.

[30] J. Lin, "Divergence measures based on the Shannon entropy," *IEEE Trans. Inf. Theory*, vol. 37, no. 1, pp. 145–151, 1991, doi: 10.1109/18.61115.

[31] O. Salem, F. Nait-Abdesselam, and A. Mehaoua, "Anomaly detection in network traffic using Jensen-Shannon divergence," in *2012 IEEE International Conference on Communications (ICC)*, IEEE, Jun. 2012, pp. 5200–5204. doi: 10.1109/ICC.2012.6364602.

[32] J. Wainer, "An empirical evaluation of imbalanced data strategies from a practitioner's point of view," *Expert Syst. Appl.*, vol. 256, p. 124863, Dec. 2024, doi: 10.1016/j.eswa.2024.124863.

[33] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Comput. Sci.*, vol. 2, no. 3, p. 160, May 2021, doi: 10.1007/s42979-021-00592-x.

[34] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, Mar. 2019, doi: 10.1016/j.comnet.2019.01.023.

[35] D. W. . Hosmer, Stanley. Lemeshow, and R. X. . Sturdivant, *Applied logistic regression*. Wiley, 2013.

[36] Vijay Kanade, "What Is Logistic Regression? Equation, Assumptions, Types, and Best Practices," spiceworks. Accessed: Mar. 10, 2026. [Online]. Available: https://www.spiceworks.com/soft-tech/what-is-logistic-regression/

[37] J. H. Friedman, “Greedy function approximation: A gradient boosting machine.,” *The Annals of Statistics*, vol. 29, no. 5, pp. 1189–1232, Oct. 2001, doi: 10.1214/aos/1013203451.

[38] R. Shwartz-Ziv and A. Armon, “Tabular Data: Deep Learning is Not All You Need,” Nov. 2021, [Online]. Available: http://arxiv.org/abs/2106.03253

[39] C. Bentéjac, A. Csörgő, and G. Martínez-Muñoz, “A comparative analysis of gradient boosting algorithms,” *Artif. Intell. Rev.*, vol. 54, no. 3, pp. 1937–1967, Mar. 2021, doi: 10.1007/s10462-020-09896-5.

[40] L. Breiman, “Bagging predictors,” *Mach. Learn.*, vol. 24, no. 2, pp. 123–140, Aug. 1996, doi: 10.1007/BF00058655.

[41] D. H. Wolpert, “Stacked Generalization,” *Neural Networks*, vol. 5, no. 2, pp. 241–259, 1992, doi: 10.1016/S0893-6080(05)80023-1.

[42] V. S. Badiger and G. K. Shyam, “A Multiclass Network Intrusion Detection System Using Stacking Ensemble Technique with Hybrid Feature Selection,” *Journal of Advances in Information Technology*, vol. 16, no. 3, pp. 342–356, 2025, doi: 10.12720/jait.16.3.342-356.

[43] R. Kohavi, “A Study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection.” Accessed: Mar. 12, 2026. [Online]. Available: https://www.researchgate.net/publication/2352264_A_Study_of_Cross-Validation_and_Bootstrap_for_Accuracy_Estimation_and_Model_Selection

[44] scikit-learn developers, “StratifiedKFold — scikit-learn documentation,” scikit-learn. Accessed: Mar. 10, 2026. [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.StratifiedKFold.html

[45] J. Snoek, H. Larochelle, and R. P. Adams, “Practical Bayesian Optimization of Machine Learning Algorithms,” in *Advances in Neural Information Processing Systems 25 (NIPS 2012)*, F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, Eds., Red Hook, NY: Curran Associates, Inc., Aug. 2012, pp. 2951–2959. Accessed: Jan. 26, 2026. [Online]. Available:

https://papers.nips.cc/paper_files/paper/2012/hash/05311655a15b75fab86956663e1819cd-Abstract.html

[46] E. Brochu, V. M. Cora, and N. de Freitas, “A Tutorial on Bayesian Optimization of Expensive Cost Functions, with Application to Active User Modeling and Hierarchical Reinforcement Learning,” Dec. 2010, [Online]. Available: http://arxiv.org/abs/1012.2599

[47] R. Turner *et al.*, “Bayesian Optimization is Superior to Random Search for Machine Learning Hyperparameter Tuning: Analysis of the Black-Box Optimization Challenge 2020,” Aug. 2021, [Online]. Available: http://arxiv.org/abs/2104.10201

[48] M. Owusu-Adjei, J. Ben Hayfron-Acquah, T. Frimpong, and G. Abdul-Salaam, “Imbalanced class distribution and performance evaluation metrics: A systematic review of prediction accuracy for determining model performance in healthcare systems,” *PLOS Digital Health*, vol. 2, no. 11, p. e0000290, Nov. 2023, doi: 10.1371/journal.pdig.0000290.

[49] M. Sokolova and G. Lapalme, “A systematic analysis of performance measures for classification tasks,” *Inf. Process. Manag.*, vol. 45, no. 4, pp. 427–437, Jul. 2009, doi: 10.1016/j.ipm.2009.03.002.

[50] E. Ficke, K. M. Schweitzer, R. M. Bateman, and S. Xu, “Analyzing Root Causes of Intrusion Detection False-Negatives: Methodology and Case Study,” Sep. 2019, [Online]. Available: http://arxiv.org/abs/1909.08725

[51] A. Sirisha and K. S. Sri, “Trust-Aware Iterative Monitoring for False Alarm Reduction in Intrusion Detection Systems,” *International Journal of Safety and Security Engineering*, vol. 15, no. 9, pp. 1909–1920, Sep. 2025, doi: 10.18280/ijsse.150914.

[52] A. Corsini, S. J. Yang, and G. Apruzzese, “On the Evaluation of Sequential Machine Learning for Network Intrusion Detection,” in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, New York, NY, USA: ACM, Aug. 2021, pp. 1–10. doi: 10.1145/3465481.3470065.