BIBLIOGRAPHY

[1] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big Data*, vol. 7, no. 1, p. 41, Dec. 2020, doi: 10.1186/s40537-020-00318-5.

[2] IBM Security, "Cost of a Data Breach Report 2024," IBM Corporation, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[3] Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine*, Cybersecurity Ventures, Nov. 13, 2020. [Online]. Available: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[4] Check Point Research Team, "Check Point Research Unveils Q2 2024 Cyber Attack Trends," *Check Point Blog*, Check Point Software Technologies, Jul. 16, 2024. [Online]. Available: https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/#:~:text=In%20Q2%202024%2C%20Check%20Point,(1%2C999%20attacks%20per%20week).

[5] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.

[6] V. Borisov, T. Leemann, K. Seßler, J. Haug, M. Pawelczyk, and G. Kasneci, "Deep Neural Networks and Tabular Data: A Survey," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 6, pp. 7499–7519, Jun. 2024, doi: 10.1109/TNNLS.2022.3229161.

[7] H. A. Alsalamah and W. N. Ismail, "A Swarm-Based Multi-Objective Framework for Lightweight and Real-Time IoT Intrusion Detection," *Mathematics*, vol. 13, no. 15, p. 2522, Aug. 2025, doi: 10.3390/math13152522.

[8] I. D. Mienye and Y. Sun, "A Survey of Ensemble Learning: Concepts, Algorithms, Applications, and Prospects," *IEEE Access*, vol. 10, pp. 99129–99149, 2022, doi: 10.1109/ACCESS.2022.3207287.

[9] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco California USA: ACM, Aug. 2016, pp. 785–794. doi: 10.1145/2939672.2939785.

[10] Á. Palma, M. Antunes, J. Bernardino, and A. Alves, "Multi-Class Intrusion Detection in Internet of Vehicles: Optimizing Machine Learning Models on Imbalanced Data," *Future Internet*, vol. 17, no. 4, p. 162, Apr. 2025, doi: 10.3390/fi17040162.

[11] S. Shekhar, A. Bansode, and A. Salim, "A Comparative study of Hyper-Parameter Optimization Tools," in *2021 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, Brisbane, Australia: IEEE, Dec. 2021, pp. 1–6. doi: 10.1109/CSDE53843.2021.9718485.

[12] O. Anser, J. François, and I. Chrisment, “Auto-tuning of Hyper-parameters for Detecting Network Intrusions via Meta-learning,” in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, Miami, FL, USA: IEEE, May 2023, pp. 1–6. doi: 10.1109/NOMS56928.2023.10154381.

[13] M. Zuraiz, M. Javed, N. Abbas, W. Abbass, W. Nawaz, and A. H. Farooqi, “Optimizing Secure and Efficient Data Aggregation in IoMT Using NSGA-II,” *IEEE Access*, vol. 13, pp. 118890–118911, 2025, doi: 10.1109/ACCESS.2025.3587016.

[14] T. Akiba, S. Sano, T. Yanase, T. Ohta, and M. Koyama, “Optuna: A Next-generation Hyperparameter Optimization Framework,” in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, Anchorage AK USA: ACM, Jul. 2019, pp. 2623–2631. doi: 10.1145/3292500.3330701.

[15] E. K. Viegas, A. O. Santin, and P. Tedeschi, “Toward a Reliable Evaluation of Machine Learning Schemes for Network-Based Intrusion Detection,” *IEEE Internet Things Mag.*, vol. 6, no. 2, pp. 70–75, Jun. 2023, doi: 10.1109/IOTM.001.2300106.

[16] M. Liang, H. T. Kassa, W. Fu, B. Coutinho, L. Feng, and C. Delimitrou, “Fine-grained Trace-driven Performance Modeling and Simulation for Large-scale ML Training,” *Proc. MLArchSys*, 2024.

[17] 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.

[18] R. S. Bora and K. Awasthi, “Real-Time Analysis Dashboard for Network Security: A systematic literature review,” *YMER*, vol. 24, no. 06, 2025.

[19] M. Luay, S. Layeghy, S. Hosseininoorbin, M. Sarhan, N. Moustafa, and M. Portmann, “Temporal Analysis of NetFlow Datasets for Network Intrusion Detection Systems,” Mar. 09, 2025, *arXiv*: arXiv:2503.04404. doi: 10.48550/arXiv.2503.04404.

[20] S. Sekhar Tripathy and B. Behera, “HYPERPARAMETER TUNING-BASED OPTIMIZED PERFORMANCE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR NETWORK INTRUSION DETECTION,” *Int. J. Netw. Secur. Its Appl.*, vol. 17, no. 6, pp. 01–26, Nov. 2025, doi: 10.5121/ijnsa.2025.17601.

[21] M. S. Al-Daweri, K. A. Zainol Ariffin, S. Abdullah, and M. F. E. Md. Senan, “An Analysis of the KDD99 and UNSW-NB15 Datasets for the Intrusion Detection System,” *Symmetry*, vol. 12, no. 10, p. 1666, Oct. 2020, doi: 10.3390/sym12101666.

[22] M. M. Abou Elasaad, S. G. Sayed, and M. M. El-Dakroury, “AegisGuard: A Multi-Stage Hybrid Intrusion Detection System with Optimized Feature Selection for Industrial IoT Security,” *Sensors*, vol. 25, no. 22, p. 6958, Nov. 2025, doi: 10.3390/s25226958.

[23] M. Al-Omari, M. Rawashdeh, F. Qutaishat, M. Alshira’H, and N. Ababneh, “An Intelligent Tree-Based Intrusion Detection Model for Cyber Security,” *J. Netw.*

Syst. Manag., vol. 29, no. 2, p. 20, Apr. 2021, doi: 10.1007/s10922-021-09591-y.
[24] M. H. L. Louk and B. A. Tama, "Dual-IDS: A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system," *Expert Syst. Appl.*, vol. 213, p. 119030, Mar. 2023, doi: 10.1016/j.eswa.2022.119030.
[25] A. Verma and V. Ranga, "Machine Learning Based Intrusion Detection Systems for IoT Applications," *Wirel. Pers. Commun.*, vol. 111, no. 4, pp. 2287–2310, Apr. 2020, doi: 10.1007/s11277-019-06986-8.
[26] S. Neupane *et al.*, "Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities," *IEEE Access*, vol. 10, pp. 112392–112415, 2022, doi: 10.1109/ACCESS.2022.3216617.
[27] S. Raschka, J. Patterson, and C. Nolet, "Machine Learning in Python: Main Developments and Technology Trends in Data Science, Machine Learning, and Artificial Intelligence," *Information*, vol. 11, no. 4, p. 193, Apr. 2020, doi: 10.3390/info11040193.
[28] M. Grandini, E. Bagli, and G. Visani, "Metrics for Multi-Class Classification: an Overview," Aug. 13, 2020, *arXiv*: arXiv:2008.05756. doi: 10.48550/arXiv.2008.05756.
[29] Md. A. Talukder *et al.*, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," *J. Big Data*, vol. 11, no. 1, p. 33, Feb. 2024, doi: 10.1186/s40537-024-00886-w.
[30] S. More, M. Idrissi, H. Mahmoud, and A. T. Asyhari, "Enhanced Intrusion Detection Systems Performance with UNSW-NB15 Data Analysis," *Algorithms*, vol. 17, no. 2, p. 64, Feb. 2024, doi: 10.3390/a17020064.
[31] S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *J. Big Data*, vol. 7, no. 1, p. 105, Dec. 2020, doi: 10.1186/s40537-020-00379-6.
[32] U. Fayyad, "From Data Mining to Knowledge Discovery in Databases".
[33] D. Singh and B. Singh, "Investigating the impact of data normalization on classification performance," *Appl. Soft Comput.*, vol. 97, p. 105524, Dec. 2020, doi: 10.1016/j.asoc.2019.105524.
[34] M. Ahsan, M. Mahmud, P. Saha, K. Gupta, and Z. Siddique, "Effect of Data Scaling Methods on Machine Learning Algorithms and Model Performance," *Technologies*, vol. 9, no. 3, p. 52, Jul. 2021, doi: 10.3390/technologies9030052.
[35] A. Tikaningsih *et al.*, "Optuna Based Hyperparameter Tuning for Improving the Performance Prediction Mortality and Hospital Length of Stay for Stroke Patients," *Telematika*, vol. 17, no. 1, pp. 1–16, Feb. 2024, doi: 10.35671/telematika.v17i1.2816.
[36] J. H. Friedman, "Greedy function approximation: A gradient boosting machine.," *Ann. Stat.*, vol. 29, no. 5, Oct. 2001, doi: 10.1214/aos/1013203451.
[37] T. Carneiro, R. V. Medeiros Da Nobrega, T. Nepomuceno, G.-B. Bian, V. H. C. De Albuquerque, and P. P. R. Filho, "Performance Analysis of Google Colaboratory as a Tool for Accelerating Deep Learning Applications," *IEEE Access*, vol. 6, pp. 61677–61685, 2018, doi: 10.1109/ACCESS.2018.2874767.

[38] D. I. Mahmood and S. M. Hameed, “A Multi-Objective Evolutionary Algorithm based Feature Selection for Intrusion Detection,” *Iraqi J. Sci.*, vol. 58, no. 1C, Apr. 2017, doi: 10.24996/ijs.2017.58.1C.16.
[39] M. A. Prabukusumo, J. Manullang, and B. Sianipar, “Particle Swarm Optimization for Multi Objective Optimization of Intrusion Detection in National Defense Cyber Infrastructure,” vol. 1, no. 1, 2025.
[40] J. Joy and M. P. Selvan, “A comprehensive study on the performance of different Multi-class Classification Algorithms and Hyperparameter Tuning Techniques using Optuna,” in *2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS)*, Kochi, India: IEEE, Jun. 2022, pp. 1–5. doi: 10.1109/IC3SIS54991.2022.9885695.
[41] J. Snoek, H. Larochelle, and R. P. Adams, “Practical Bayesian Optimization of Machine Learning Algorithms,” Aug. 29, 2012, *arXiv*: arXiv:1206.2944. doi: 10.48550/arXiv.1206.2944.
[42] 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)*, Orlando, FL, USA: IEEE, Dec. 2021, pp. 5413–5419. doi: 10.1109/BigData52589.2021.9671576.
[43] J. Demsˇar and J. Demsar, “Statistical Comparisons of Classifiers over Multiple Data Sets”.