REFERENCES

[1] S. K. Rajamani and R. S. Iyer, "Networks in healthcare: A systematic review," pp. 391–404, 6 2023.

[2] M. Pagani and C. Pardo, "The impact of digital technology on relationships in a business network," *Industrial Marketing Management*, vol. 67, pp. 185–192, 11 2017.

[3] U. Madhow, *Fundamentals of digital communication*. Cambridge University Press, 2008.

[4] M. Schmitt, "Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (ai)-enabled malware and intrusion detection," *Journal of Industrial Information Integration*, vol. 36, 12 2023.

[5] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 11 2021.

[6] H. J. Liao, C. H. R. Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," pp. 16–24, 1 2013.

[7] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," in *Procedia Computer Science*, vol. 185. Elsevier B.V., 2021, pp. 239–247.

[8] R. A. Abed, E. K. Hamza, and A. J. Humaidi, "A modified cnn-ids model for enhancing the efficacy of intrusion detection system," *Measurement: Sensors*, vol. 35, 10 2024, cool paper.

[9] M. Azizjon, A. Jumabek, and W. Kim, "1d cnn based network intrusion detection with normalization on imbalanced data," in *2020 International Conference on Artificial Intelligence in Information and Communication, ICAIIC 2020*. Institute of Electrical and Electronics Engineers Inc., 2 2020, pp. 218–224.

[10] E. Ozdogan, "A comprehensive analysis of the machine learning algorithms in iot ids systems," *IEEE Access*, vol. 12, pp. 46 785–46 811, 2024.

[11] D. Sudyana, Y.-D. Lin, M. Verkerken, R.-H. Hwang, Y.-C. Lai, L. D'Hooge, T. Wauters, B. Volckaert, and F. D. Turck, "Improving generalization of ml-based ids with lifecycle-based dataset, auto-learning features, and deep learning," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, pp. 645–662, 5 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10531223/

[12] V. Ravi, "Deep learning-based network intrusion detection in smart healthcare enterprise systems," *Multimedia Tools and Applications*, vol. 83, pp. 39 097–39 115, 4 2024.

[13] S. Biswas and M. S. A. Ansari, "Securing iot networks in cloud computing environments: a real-time ids," *Journal of Supercomputing*, vol. 80, pp. 14 489–14 519, 7 2024.

[14] C. Park, J. Lee, Y. Kim, J.-G. Park, H. Kim, and D. Hong, "An enhanced ai-based network intrusion detection system using generative adversarial networks," *IEEE Internet of Things Journal*, vol. 10, pp. 2330–2345, 2 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9908159/

[15] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "Cnn-based network intrusion detection against denial-of-service attacks," *Electronics (Switzerland)*, vol. 9, pp. 1–21, 6 2020.

[16] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "Ddos attack detection and classification via convolutional neural network (cnn)," in *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*. IEEE, 12 2019, pp. 233–238. [Online]. Available: https://ieeexplore.ieee.org/document/9014826/

[17] D. Aksu, S. Üstebay, M. A. Aydin, and T. Atmaca, "Intrusion detection with comparative analysis of supervised learning techniques and fisher score feature selection algorithm," in *Communications in Computer and Information Science*, vol. 935. Springer Verlag, 2018, pp. 141–149.

[18] S. Salmi and L. Oughdir, "Cnn-lstm based approach for dos attacks detection in wireless sensor networks," p. 2022, 2022. [Online]. Available: www.ijacsa.thesai.org

[19] W.-L. Chu, C.-J. Lin, and K.-N. Chang, "Detection and classification of advanced persistent threats and attacks using the support vector

machine," *Applied Sciences*, vol. 9, p. 4579, 10 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/21/4579

[20] Z. Zhang and P. Pan, "A hybrid intrusion detection method based on improved fuzzy c-means and support vector machine," in *Proceedings - 2019 International Conference on Communications, Information System, and Computer Engineering, CISCE 2019*. Institute of Electrical and Electronics Engineers Inc., 7 2019, pp. 210–214.

[21] Amarudin, R. Ferdiana, and Widyawan, "A systematic literature review of intrusion detection system for network security: Research trends, datasets and methods," in *ICICoS 2020 - Proceeding: 4th International Conference on Informatics and Computational Sciences*. Institute of Electrical and Electronics Engineers Inc., 11 2020.

[22] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks," *Future Internet*, vol. 12, 3 2020.

[23] R. Panigrahi, S. Borah, A. K. Bhoi, M. F. Ijaz, M. Pramanik, Y. Kumar, and R. H. Jhaveri, "A consolidated decision tree-based intrusion detection system for binary and multiclass imbalanced datasets," *Mathematics*, vol. 9, 4 2021.

[24] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine," *Electronics (Switzerland)*, vol. 9, 1 2020.

[25] T. Wisanwanichthan and M. Thammawichai, "A double-layered hybrid approach for network intrusion detection system using combined naive bayes and svm," *IEEE Access*, vol. 9, pp. 138 432–138 450, 2021.

[26] L. Chen, X. Kuang, A. Xu, S. Suo, and Y. Yang, "A novel network intrusion detection system based on cnn," in *Proceedings - 2020 8th International Conference on Advanced Cloud and Big Data, CBD 2020*. Institute of Electrical and Electronics Engineers Inc., 12 2020, pp. 243–247.

[27] R. U. Khan, X. Zhang, M. Alazab, and R. Kumar, "An improved convolutional neural network model for intrusion detection in networks," in *Proceedings - 2019 Cybersecurity and Cyberforensics Conference, CCC 2019*. Institute of Electrical and Electronics Engineers Inc., 5 2019, pp. 74–77.

[28] M. Verkerken, L. D'hooge, T. Wauters, B. Volckaert, and F. D. Turck, "Towards model generalization for intrusion detection: Unsupervised machine learning techniques," *Journal of Network and Systems Management*, vol. 30, 1 2022.

[29] K. A. Jallad, M. Aljnidi, and M. S. Desouki, "Anomaly detection optimization using big data and deep learning to reduce false-positive," *Journal of Big Data*, vol. 7, 12 2020.

[30] S. Bagui and K. Li, "Resampling imbalanced data for network intrusion detection datasets," *Journal of Big Data*, vol. 8, 12 2021.

[31] P. W. Singer and A. Friedman, *Cybersecurity and cyberwar : what everyone needs to know*. Oxford University Press, 2014.

[32] R. Palanisamy, A. A. Norman, and M. L. M. Kiah, "Compliance with bring your own device security policies in organizations: A systematic literature review," *Computers and Security*, vol. 98, 11 2020.

[33] A. T. A. M, A. W. A. Wahab, and M. Y. I. Idris, "Systematic literature review on security access control policies and techniques based on privacy requirements in a byod environment: State of the art and future directions," 7 2023.

[34] J. Jabez and B. Muthukumar, "Intrusion detection system (ids): Anomaly detection using outlier detection approach," in *Procedia Computer Science*, vol. 48. Elsevier B.V., 2015, pp. 338–346.

[35] Q. S. Qassim, A. M. Zin, M. Juzaiddin, and A. Aziz, "Anomalies classification approach for network-based intrusion detection system," pp. 1159–1172, 2016.

[36] M. Ozkan-Okay, R. Samet, O. Aslan, and D. Gupta, "A comprehensive systematic literature review on intrusion detection systems," pp. 157 727–157 760, 2021.

[37] Z. Wang, Y. Liu, D. He, and S. Chan, "Intrusion detection methods based on integrated deep learning model," *Computers and Security*, vol. 103, 4 2021.

[38] D. E. Denning, "An intrusion-detection model," in *1986 IEEE Symposium on Security and Privacy*, 1986, pp. 118–118.

[39] T. F. Lunt, "Ides: An intelligent system for detecting intruders," in *Proceedings of the Symposium: Computer Security, Threat and Countermeasures*, November 1990.

[40] S. O. Arik and T. Pfister, "Tabnet: Attentive interpretable tabular learning," 8 2019. [Online]. Available: http://arxiv.org/abs/1908.07442

[41] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," 12 2015. [Online]. Available: http://arxiv.org/abs/1512.03385

[42] S. Lai, L. Xu, K. Liu, and J. Zhao, "Recurrent convolutional neural networks for text classification." [Online]. Available: www.aaai.org

[43] D. Amodei, R. Anubhai, E. Battenberg, C. Case, J. Casper, B. Catanzaro, J. Chen, M. Chrzanowski, A. Coates, G. Diamos, E. Elsen, J. Engel, L. Fan, C. Fougner, T. Han, A. Hannun, B. Jun, P. LeGresley, L. Lin, S. Narang, A. Ng, S. Ozair, R. Prenger, J. Raiman, S. Satheesh, D. Seetapun, S. Sengupta, Y. Wang, Z. Wang, C. Wang, B. Xiao, D. Yogatama, J. Zhan, and Z. Zhu, "Deep speech 2: End-to-end speech recognition in english and mandarin," 12 2015. [Online]. Available: http://arxiv.org/abs/1512.02595

[44] B. Allison, D. Guthrie, and L. Guthrie, "Lnai 4188 - another look at the data sparsity problem."

[45] B. Becker and R. Kohavi, "Adult," UCI Machine Learning Repository, 1996, DOI: https://doi.org/10.24432/C5XW20.

[46] M. Dehmer and S. C. Basak, *Statistical and machine learning approaches for network analysis*. Wiley, 2012.

[47] F. Emmert-Streib, S. Moutari, and M. Dehmer, *Elements of Data Science, Machine Learning, and Artificial Intelligence Using R*. Springer International Publishing, 2023. [Online]. Available: https://link.springer.com/10.1007/978-3-031-13339-8

[48] T. Gowda, W. You, C. Lignos, and J. May, "Macro-average: Rare types are important too," pp. 1138–1157. [Online]. Available: https://github.com/isi-nlp/sacrebleu/tree/

[49] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proceedings of the 4th International Conference on Information Systems*

Security and Privacy - ICISSP, INSTICC. SciTePress, 2018, pp. 108–116. [Online]. Available: https://www.scitepress.org/Link.aspx?doi=10.5220/0006639801080116

[50] C. I. of Cybersecurity. (2018) Intrusion detection evaluation dataset (cic-ids2017). [Accessed: 10 April 2025]. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html

[51] H. K. Bui, Y. D. Lin, R. H. Hwang, P. C. Lin, V. L. Nguyen, and Y. C. Lai, "Creme: A toolchain of automatic dataset collection for machine learning in intrusion detection," *Journal of Network and Computer Applications*, vol. 193, 11 2021.

[52] F. Yudha, "CREMEv2," https://github.com/masjohncook/CREMEv2, 3 2023.