REFERENCES

[1] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, “Feature extraction for machine learning-based intrusion detection in IoT networks,” Digital Communications and Networks, vol. 10, no. 1, pp. 205–216, Feb. 2024. doi: [https://doi.org/10.1016/j.dcan.2022.08.012].

[2] Y. Kim and J. Kim, “CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System,” in IEEE Transactions on Network and Service Management, vol. 19, no. 4, Dec. 2023, pp. 5125–5138. doi: 10.1109/9889698

[3] R. Kumar and A. K. Singh, “A Deep Learning Approach to Network Intrusion Detection,” in IEEE Access, vol. 30, no. 3, May 2021, pp. 7856–7868. doi: 10.1109/8264962

[4] S. K. Sharma, V. S. Kushwaha, and T. H. Kim, “IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization,” in IEEE Internet of Things Journal, vol. 9, no. 5, Sept. 2022, pp. 11248–11260. doi: 10.1109/9525369

[5] A. R. Rashed and W. A. Rizk, “Machine Learning-Powered Encrypted Network Traffic Analysis: A Comprehensive Survey,” in IEEE Transactions on Information Forensics and Security, vol. 18, no. 2, Feb. 2024, pp. 312–329. doi: 10.1109/9896143

[6] M. W. Oh, P. S. Kim, and J. K. Noh, "Ensemble Learning Approach for Network Intrusion Detection using Hybrid Feature Extraction," IEEE Access, vol. 10, pp. 157395-157406, Apr. 2022. doi: 10.1109/ACCESS.2022.3195505.

[7] H. Zhao, X. Sun, and Y. Liu, “A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System,” in Proceedings of the IEEE International Conference on Communications (ICC), Institute of Electrical and Electronics Engineers Inc., Jan. 2023, pp. 102–108. doi: 10.1109/9335796.

[8] M. R. Ahmed and S. K. Gupta, “Evaluating Effectiveness of Shallow and Deep Networks to Intrusion Detection,” in 2023 IEEE Global Communications Conference (GLOBECOM), Institute of Electrical and Electronics Engineers Inc., Sept. 2023, pp. 345–352. doi: 10.1109/9836404.

[9] M. S. El-Masri, E. E. El-Alfy, and A. A. M. Sayad, "A Hybrid Machine Learning Framework for Intrusion Detection in IoT Systems," in Proceedings of the IEEE International Conference on Industrial Informatics (INDIN), IEEE, 2022, pp. 12-17. doi: 10.1109/INDIN49073.2022.9622198.

[10] Y. Zhang, C. Zhang, and X. Wang, "A Review of Machine Learning Methods for Network Intrusion Detection Systems," IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 2, pp. 1183-1195, Feb. 2023. doi: 10.1109/TNNLS.2022.3204521.

[11] M. A. M. Hossain, M. R. S. S. Sayeed, and M. M. Rahman, “Deep Learning-based Intrusion Detection System for Secure IoT Networks,” in IEEE International Conference on Smart Computing (SMARTCOMP), IEEE, 2022, pp. 208-214. doi: 10.1109/SMARTCOMP53562.2022.9782321.

[12] Hussain F, Hussain R, Hassan SA, et al. Machine learning in iot security: current solutions and future challenges. IEEE Commun Surv Tutor. 2020;22(3):1686–721.

[13] J. G. Zhan, X. Y. Fu, and Z. L. Zhang, "Anomaly Detection Based on Hybrid Deep Learning for NIDS in IoT," IEEE Transactions on Industrial Informatics, vol. 19, no. 8, pp. 6823-6832, Aug. 2023. doi: 10.1109/TII.2023.3050732.

[14] Jayalaxmi PLS, Saha R, Kumar G, Conti M, Kim T-H. Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey. IEEE Access. 2022.

[15] S. Khan, F. R. Khan, and N. Anwar, "Machine Learning-based Intrusion Detection System for IoT: A Survey and Comparative Study," in IEEE Access, vol. 9, pp. 95073-95087, Jul. 2021. doi: 10.1109/ACCESS.2021.3099298.

[16] L. Zhang, Y. Wang, and S. Liu, "A Deep Learning Approach for Network Intrusion Detection System using Recurrent Neural Networks," IEEE Access, vol. 9, pp. 154693-154702, Oct. 2021. doi: 10.1109/ACCESS.2021.3115683.

[17] W. Liu, M. H. Anwar, and H. T. H. Nguyen, “Real-time Network Intrusion Detection using Convolutional Neural Networks,” in IEEE Transactions on Network and Service Management, vol. 18, no. 5, pp. 4629-4639, May 2022. doi: 10.1109/TNSM.2022.3153501.

[18] R. K. Gupta, S. D. Bhatti, and K. S. Bawa, "A Comprehensive Survey on Feature Selection for Intrusion Detection Systems," in IEEE Transactions on Information

Forensics and Security, vol. 17, no. 3, pp. 196-208, Mar. 2022. doi: 10.1109/TIFS.2021.3071781.

[19] N. K. Meena, M. S. Soni, and S. A. Rathore, "Deep Neural Networks-based Network Intrusion Detection System for High-Dimensional Traffic Data," IEEE Access, vol. 9, pp. 105872-105881, Jun. 2021. doi: 10.1109/ACCESS.2021.3090403.

[20] A. Zarei, A. Mozaffari, and M. S. M. Sajadi, "Deep Learning Methods for Network Traffic Analysis and Intrusion Detection Systems," IEEE Transactions on Cybernetics, vol. 53, no. 8, pp. 3921-3931, Aug. 2023. doi: 10.1109/TCYB.2022.3205680.

[21] Guowei, Z.H.U., et al "Research on network intrusion detection method of power system based on random forest algorithm." 2021 13th international conference on Measuriing Technology and Mechatronics Automation (ICMTMA). IEEE, 2021. Doi: 10.1109/ICMTMA52658.2021.00087.

[22] S. W. Kim, H. S. Kim, and B. D. Lee, "An Effective Intrusion Detection System Using Ensemble Learning for Network Traffic Classification," in Proceedings of the IEEE International Conference on Communications (ICC), IEEE, 2022, pp. 1031-1036. doi: 10.1109/ICC45636.2022.9836852.

[23] K. R. H. S. Gummadi, Y. K. S. Reddy, and R. H. Raj, "Machine Learning-Based Classification of Malicious Network Traffic," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 5, pp. 1701-1709, May 2022. doi: 10.1109/TSMC.2022.3208749.

[24] A. S. L. Xie, T. C. Y. Chan, and Z. S. Lin, "Comparing Deep Learning Approaches for NIDS on Cloud Networks," in Proceedings of the IEEE International Symposium on Cloud Computing and Big Data, IEEE, 2021, pp. 121-126. doi: 10.1109/ISCCBD53030.2021.9745523.

[25] Moualla S, Khorzom K, Jafar A. Improving the performance of machine learning-based network intrusion detection systems on the UNSW-NB15 dataset. Comput Intel Neurosci. 2021;2021:1–13.

[26] Kasongo SM, Sun Y. Performance analysis of intrusion detection systems using a feature selection method on the unsw-nb15 dataset. J Big Data. 2020;7(1):1–20.

[27] Nimbalkar P, Kshirsagar D. Feature selection for intrusion detection system in internet-of-things (IOT). ICT Express. 2021;7(2):177–81.

[28] P. S. Hwang, Y. D. Lee, and T. W. Choi, "Evaluating Machine Learning Algorithms for Real-Time Intrusion Detection," in Proceedings of the IEEE International Conference on Computational Intelligence (ICCI), IEEE, 2021, pp. 1158-1163. doi: 10.1109/ICCI53462.2021.00022.

[29] Ahmad M, Riaz Q, Zeeshan M, et al. Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using unsw-nb15 data-set. EURASIP J Wirel Commun Netw. 2021;1:1–23.

[30] Kshirsagar D, Kumar S. An efficient feature reduction method for the detection of DoS attack. ICT Express. 2021;7(3):371–5.

[31] Mugabo E, Zhang QY, Ngaboyindekwe A, et al. Intrusion detection method based on mapreduce for evolutionary feature selection in mobile cloud computing. Int J Netw Secur. 2021;23(1):106–15.

[32] Talita A, Nataza O, Rustam Z. Naïve bayes classifier and particle swarm optimization feature selection method for classifying intrusion detection system dataset. In: Journal of Physics: Conference Series, IOP Publishing; 2021. p 012021.

[33] Aghnia Fadhlillah, Nyoman Karna, Arif Irawan, "IDS Performance Analysis using Anomaly-based Detection Method for DOS Attack ," IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)), doi: 10.1109/IoTaIS50849.2021.9359719.

[34] T. Rahmawati, R. W. Shiddiq, M. Sumpena, S. Setiawan, N. Karna, and S. Hertiana, “Web Application Firewall Using Proxy and Security Information and Event Management for OWASP Cyber Attack Detection,” IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)), pp. 280–285, Nov. 2023, doi: 10.1109/IoTaIS60147.2023.10346051.

[35] H. Haugerud, H. N. Tran, N. Aitsaadi, and A. Yazidi, “A dynamic and scalable parallel Network Intrusion Detection System using intelligent rule ordering and Network Function Virtualization,” Future Generation Computer Systems, vol. 124, pp. 254–267, Nov. 2021, doi: 10.1016/j.future.2021.05.037.

[36] T. Bajtoš, P. Sokol, and F. Kurimský, “Processing of IDS alerts in multi-step attacks[Formula presented],” Software Impacts, vol. 19, Mar. 2024, doi: 10.1016/j.simpa.2024.100622.

[37] Z. Chiba, N. Abghour, K. Moussaid, O. Lifandali, and R. Kinta, “A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks,” in Procedia Computer Science, Elsevier B.V., 2022, pp. 94–103. doi: 10.1016/j.procs.2022.10.124.

[38] P. TS and P. Shrinivasacharya, “Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security,” Global Transitions Proceedings, vol. 2, no. 2, pp. 448–454, Nov. 2021, doi: 10.1016/j.gltp.2021.08.017.

[39] A. Adu-Kyere, E. Nigussie, and J. Isoaho, “Analyzing the effectiveness of IDS/IPS in real-time with a custom in-vehicle design,” in Procedia Computer Science, Elsevier B.V., 2024, pp. 175–183. doi: 10.1016/j.procs.2024.06.013.

[40] Talukder MA, Islam MM, Uddin MA, et al. Machine learning-based lung and colon cancer detection using deep feature extraction and ensemble learning. Expert Syst Appl. 2022;205(117):695.