Daftar Pustaka

[1] P. A and S. S, "DDOS ATTACK DETECTION IN TELECOMMUNICATION NETWORK USING MACHINE LEARNING," *Journal of Ubiquitous Computing and Communication Technologies*, vol. 01, no. 01, pp. 33–44, Sep. 2019, doi: 10.36548/jucct.2019.1.004.

[2] F. J. Abdullayeva, "Distributed denial of service attack detection in E-government cloud via data clustering," *Array*, vol. 15, Sep. 2022, doi: 10.1016/j.array.2022.100229.

[3] P. Khuphiran, P. Leelaprute, P. Uthayopas, K. Ichikawa, and W. Watanakeesuntorn, "Performance Comparison of Machine Learning Models for DDoS Attacks Detection," in *2018 22nd International Computer Science and Engineering Conference (ICSEC)*, IEEE, Nov. 2018, pp. 1–4. doi: 10.1109/ICSEC.2018.8712757.

[4] "Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper - Cisco." Accessed: Mar. 30, 2023. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[5] F. J. Abdullayeva, "Convolutional Neural Network-Based Automatic Diagnostic System for AL-DDoS Attacks Detection," *International Journal of Cyber Warfare and Terrorism*, vol. 12, no. 1, pp. 1–15, Jul. 2022, doi: 10.4018/IJCWT.305242.

[6] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.

[7] P. K. Kishore, S. Ramamoorthy, and V. N. Rajavarman, "AN IMPROVED BIO-INSPIRED BAT ALGORITHM FOR DETECTION AND PREVENTION OF HTTP FLOOD DDOS ATTACK USING MACHINE LEARNING METRICS," 2020.

[8] H. S. Obaid and E. H. Abeed, "Abeed,-DoS and DDoS Attacks at OSI Layers," *International Journal of Multidisciplinary Research and Publications Hadeel S. Obaid and Esamaddin H*, vol. 2, no. 8, pp. 1–9, 2020.

[9] M. S. Mahmoud and Y. Xia, "Distributed denial-of-service attacks," in *Cloud Control Systems*, S. Ison, Ed., Elsevier, 2020, pp. 51–76. doi: 10.1016/B978-0-12-818701-2.00011-1.

[10] B. Nugraha and R. N. Murthy, "Deep Learning-based Slow DDoS Attack Detection in SDN-based Networks," in *2020 IEEE Conference on Network*

Function Virtualization and Software Defined Networks, NFV-SDN 2020 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 51–56. doi: 10.1109/NFV-SDN50289.2020.9289894.

[11] P. Karthika and K. Arockiasamy, "Simulation of SDN in mininet and detection of DDoS attack using machine learning," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 3, pp. 1797–1805, Jun. 2023, doi: 10.11591/eei.v12i3.5232.

[12] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," in *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/INMIC50486.2020.9318216.

[13] H. Majed, H. N. Noura, O. Salman, M. Malli, and A. Chehab, "Efficient and secure statistical DDoS detection scheme," in *ICETE 2020 - Proceedings of the 17th International Joint Conference on e-Business and Telecommunications*, SciTePress, 2020, pp. 153–161. doi: 10.5220/0009873801530161.

[14] S. Hosseini and M. Azizi, "The hybrid technique for DDoS detection with supervised learning algorithms," *Computer Networks*, vol. 158, pp. 35–45, Jul. 2019, doi: 10.1016/j.comnet.2019.04.027.

[15] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, "A survey on deep learning for big data," Jul. 01, 2018, *Elsevier B.V.* doi: 10.1016/j.inffus.2017.10.006.

[16] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.

[17] A. Aljuhani, "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," *IEEE Access*, vol. 9, pp. 42236–42264, 2021, doi: 10.1109/ACCESS.2021.3062909.

[18] Naveen Bindra and Manu Sood, "Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset," *Automatic Control and Computer Sciences*, vol. 53, no. 5, pp. 419–428, Sep. 2019, doi: 10.3103/S0146411619050043.

[19] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via Convolutional Neural Network (CNN)," *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS).*

[20] A. Voulodimos, N. Doulamis, A. Doulamis, and E. Protopapadakis, “Deep Learning for Computer Vision: A Brief Review,” 2018, *Hindawi Limited*. doi: 10.1155/2018/7068349.

[21] *2018 International Conference on Computing, Power and Communication Technologies (GUCON).* IEEE, 2018.

[22] P. P. Shinde, *A Review of Machine Learning and Deep Learning Applications*.

[23] C. Janiesch, P. Zschech, and K. Heinrich, “Machine learning and deep learning”, doi: 10.1007/s12525-021-00475-2/Published.

[24] T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, *Machine Learning Approaches in Cyber Security Analytics*. Singapore: Springer Singapore, 2020. doi: 10.1007/978-981-15-1706-8.

[25] C. Janiesch, P. Zschech, and K. Heinrich, “Machine learning and deep learning,” *The International Journal On Networked Bussines*, vol. 31, pp. 685–695, 2021, doi: 10.1007/s12525-021-00475-2/Published.

[26] N. Buduma and N. Locascio, “Deep Learning DESIGNING NEXT-GENERATION MACHINE INTELLIGENCE ALGORITHMS Nikhil Buduma with contributions by Nicholas Locascio,” 2017.

[27] L. L. Minku, G. Cabral, M. Martins, and M. Wagner, “Introduction to Computational Intelligence,” vol. 1, pp. 105–110, 2023, doi: 10.5281/zenodo.7537827.

[28] E. Bisong, *Building Machine Learning and Deep Learning Models on Google Cloud Platform*. Apress, 2019. doi: 10.1007/978-1-4842-4470-8.

[29] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, “A Survey on Machine Learning Techniques for Cyber Security in the Last Decade,” *IEEE Access*, vol. 8, pp. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[30] G. Howser, *Computer Networks and the Internet*. Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-34496-2.

[31] C. Panek, *Networking fundamentals*. Canada: John Wiley & Sons, Inc, 2020.

[32] L. Yang, B. Ng, W. K. G. Seah, L. Groves, and D. Singh, “A survey on network forwarding in Software-Defined Networking,” Feb. 15, 2021, *Academic Press*. doi: 10.1016/j.jnca.2020.102947.

[33] S. Saraswat, V. Agarwal, H. P. Gupta, R. Mishra, A. Gupta, and T. Dutta, “Challenges and solutions in Software Defined Networking: A survey,” *Journal of Network and Computer Applications*, vol. 141, pp. 23–58, Sep. 2019, doi: 10.1016/j.jnca.2019.04.020.

[34] P. Ferdiansyah and U. Amikom Yogyakarta, “Analisis Perbandingan Parameter QoS Standar TIPHON Pada Jaringan Nirkabel Dalam Penerapan Metode PCQ,” 2022.

[35] R. A. R. Q. Y. Putri, Anhar, and A. Al Nazen, “Analysis of LTE Network Quality of Service on Streaming Application,” *International Joournal of Electrical, Energy and Power System Engineering (IJEEPSE)*, vol. 6, no. 2, pp. 151–155, 2023.

[36] M. Snehi and A. Bhandari, “Vulnerability retrospection of security solutions for software-defined Cyber-Physical System against DDoS and IoT-DDoS attacks,” May 01, 2021, *Elsevier Ireland Ltd*. doi: 10.1016/j.cosrev.2021.100371.

[37] 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, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[38] A. M. Abdul and S. Umar, “Attacks of Denial-of-Service on Networks Layer of OSI Model and Maintaining of Security,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 5, no. 1, pp. 181–186, 2017, doi: 10.11591/ijeecs.v5.i1.pp.

[39] S. Pande, A. Khamparia, D. Gupta, and D. N. H. Thanh, “DDOS Detection Using Machine Learning Technique,” 2021, pp. 59–68. doi: 10.1007/978-981-15-8469-5_5.

[40] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, “IoT DoS and DDoS Attack Detection using ResNet,” in *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/INMIC50486.2020.9318216.

[41] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, “Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods,” *IEEE Access*, vol. 7, pp. 51691–51713, 2019, doi: 10.1109/ACCESS.2019.2908998.

[42] A. Bhati, A. Bouras, U. Ahmed Qidwai, and A. Belhi, “Deep learning based identification of DDoS attacks in industrial application,” in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, IEEE, Jul. 2020, pp. 190–196. doi: 10.1109/WorldS450073.2020.9210320.

[43] “Hacktivists step back giving way to professionals: a look at DDoS in Q3 2022 | Kaspersky.” Accessed: May 03, 2023. [Online]. Available: https://www.kaspersky.com/about/press-releases/2022_hacktivists-step-back-giving-way-to-professionals-a-look-at-ddos-in-q3-2022

[44] J. A. Perez-Diaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, “A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning,” *IEEE Access*, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[45] S. H. Islam, P. Vijayakumar, M. Z. A. Bhuiyan, R. Amin, V. Rajeev M., and B. Balusamy, “A Provably Secure Three-Factor Session Initiation Protocol for Multimedia Big Data Communications,” *IEEE Internet Things J*, vol. 5, no. 5, pp. 3408–3418, Oct. 2018, doi: 10.1109/JIOT.2017.2739921.

[46] 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, Dec. 2019, pp. 233–238. doi: 10.1109/ICICIS46948.2019.9014826.

[47] M. S. Khaing, Y. M. Thant, T. Tun, C. S. Htwe, and M. M. S. Thwin, “IoT Botnet Detection Mechanism Based on UDP Protocol,” in *2020 IEEE Conference on Computer Applications(ICCA)*, IEEE, Feb. 2020, pp. 1–7. doi: 10.1109/ICCA49400.2020.9022832.

[48] “Top 10 Python Libraries untuk Machine Learning - Algoritma.” Accessed: Apr. 27, 2023. [Online]. Available: https://algorit.ma/blog/python-libraries-machine-learning-2022/

[49] N. K. Manaswi, *Deep Learning with Applications Using Python*. Berkeley, CA: Apress, 2018. doi: 10.1007/978-1-4842-3516-4.

[50] Y. Cui *et al.*, “Towards DDoS detection mechanisms in Software-Defined Networking,” Sep. 15, 2021, *Academic Press*. doi: 10.1016/j.jnca.2021.103156.

[51] Institute of Electrical and Electronics Engineers, *2020 IEEE International Conference on Communications Workshops (ICC) : proceedings : Dublin, Ireland, 7-11 June 2020.* 2020.

[52] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, “Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN,” *Future Generation Computer Systems*, vol. 111, pp. 763–779, Oct. 2020, doi: 10.1016/j.future.2019.10.015.