DAFTAR PUSTAKA

[1] M. Roopak, G. Y. Tian, and Chambers Jonathon, "An Intrusion Detection System Against DDoS Attacks in loT Networks," in *10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas: IEEE, 2020, pp. 562–567. doi: 10.1109/CCWC47524.2020.9031206.

[2] S. S. Bhunia and M. Gurusamy, "Dynamic Attack Detection and Mitigation in IoT using SDN," in *27th International Telecommunication Networks and Applications Conference (ITNAC)*, Melbourne: IEEE, 2017. doi: 10.1109/ATNAC.2017.8215418.

[3] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating IoT Device based DDoS Attacks using Blockchain," in *CRYBLOCK 2018 - Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Part of MobiSys 2018: The 16th Annual International Conference on Mobile Systems, Applications, and Services*, Association for Computing Machinery, Inc, Jun. 2018, pp. 71–76. doi: 10.1145/3211933.3211946.

[4] L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Deep Transfer Learning for IoT Attack Detection," *IEEE Access*, vol. 8, pp. 107335–107344, 2020, doi: 10.1109/ACCESS.2020.3000476.

[5] J. Bhayo, R. Jafaq, A. Ahmed, S. Hameed, and S. A. Shah, "A Time-Efficient Approach Toward DDoS Attack Detection in IoT Network Using SDN," *IEEE Internet Things J*, vol. 9, no. 5, pp. 3612–3630, Mar. 2022, doi: 10.1109/JIOT.2021.3098029.

[6] D. K. Sharma *et al.*, "Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks," *Ad Hoc Networks*, vol. 121, Oct. 2021, doi: 10.1016/j.adhoc.2021.102603.

[7] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 6, no. 1, pp. 172–180, 2022, [Online]. Available: http://j-ptiik.ub.ac.id

[8] Harshita, "Detection and Prevention of ICMP Flood DDOS Attack," *International Journal of New Technology and Research (IJNTR)*, vol. 3, no. 3, pp. 63–69, 2017, [Online]. Available: www.ijntr.org

[9] V. Chauhan and P. Saini, "ICMP flood attacks: A vulnerability analysis," in *Advances in Intelligent Systems and Computing*, Springer Verlag, 2018, pp. 261–268. doi: 10.1007/978-981-10-8536-9_26.

[10] E. Hodo *et al.*, "Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System," in *International Symposium on Networks, Computers and Communications (ISNCC)*, Yasmine Hammamet: [IEEE], 2016. doi: 10.1109/ISNCC.2016.7746067.

[11] M. Aamir and S. M. Ali Zaidi, "Clustering based semi-supervised machine learning for DDoS attack classification," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 4, pp. 436–446, May 2021, doi: 10.1016/j.jksuci.2019.02.003.

[12] E. O. Nasution and A. Basuki, "Implementasi Algoritme C5.0 Untuk Klasifikasi Serangan DDoS," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 1, pp. 389–395, 2021, [Online]. Available: http://j-ptiik.ub.ac.id

[13] H. Polat, O. Polat, and A. Cetin, "Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models," *Sustainability (Switzerland)*, vol. 12, no. 3, pp. 1–16, Feb. 2020, doi: 10.3390/su12031035.

[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] K. Kurniabudi, A. Harris, and V. Veronica, "Komparasi Performa Tree-Based Classifier Untuk Deteksi Anomali Pada Data Berdimensi Tinggi dan Tidak Seimbang," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 1, p. 370, Jan. 2022, doi: 10.30865/mib.v6i1.3473.

[16] K. Kurniabudi, A. Harris, and A. E. Mintaria, "Komparasi Information Gain, Gain Ratio, CFs-Bestfirst dan CFs-PSO Search Terhadap Performa Deteksi Anomali," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 5, no. 1, p. 332, Jan. 2021, doi: 10.30865/mib.v5i1.2258.

[17] M. S. El Sayed, N. A. Le-Khac, M. A. Azer, and A. D. Jurcut, "A Flow-Based Anomaly Detection Approach with Feature Selection Method Against DDoS Attacks in SDNs," *IEEE Trans Cogn Commun Netw*, vol. 8, no. 4, pp. 1862–1880, Dec. 2022, doi: 10.1109/TCCN.2022.3186331.

[18] Y. Chen, J. Hou, Q. Li, and H. Long, "DDoS Attack Detection Based on Random Forest," in *International Conference on Progress in Informatics and Computing (PIC)*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 328–334. doi: 10.1109/PIC50277.2020.9350788.

[19] L. Ikhwanul Uzlah, R. Adi Saputra, and Isnawaty, "DETEKSI SERANGAN SIBER PADA JARINGAN KOMPUTER MENGGUNAKAN METODE RANDOM FOREST," *Jurnal Mahasiswa Teknik Informatika*, vol. 8, no. 3, pp. 2787–2793, Jun. 2024, doi: https://doi.org/10.36040/jati.v8i3.8891.

[20] S. Sivaranjani, S. Ananya, J. Aravinth, and R. Karthika, "Diabetes Prediction using Machine Learning Algorithms with Feature Selection and Dimensionality Reduction," in *7th International Conference on Advanced Computing and Communication Systems (ICACCS))*, Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 141–146. doi: 10.1109/ICACCS51430.2021.9441935.

[21] Kurniabudi, A. Harris, and A. Rahim, "Seleksi Fitur dengan Information Gain untuk Meningkatkan Deteksi Serangan DDoS Menggunakan Random Forest," *Techno.COM*, vol. 19, no. 1, pp. 56–66, 2020, doi: https://doi.org/10.33633/tc.v19i1.2860.

[22] P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, Jul. 2018, doi: 10.1016/j.jksuci.2016.10.003.

[23] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, and J. Qin, "A survey on application of machine learning for Internet of Things," *International Journal of Machine*

Learning and Cybernetics, vol. 9, no. 8, pp. 1399–1417, Aug. 2018, doi: 10.1007/s13042-018-0834-5.

[24] S. Villamil, C. Hernández, and G. Tarazona, "An Overview of Internet of Things," *Telkomnika (Telecommunication, Computing, Electronics and Control)*, vol. 18, no. 5, pp. 2320–2327, Oct. 2020, doi: 10.12928/TELKOMNIKA.v18i5.15911.

[25] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, "Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach," *Sensors*, vol. 20, no. 3, pp. 1–18, Feb. 2020, doi: 10.3390/s20030816.

[26] G. H. Sandi and Y. Fatma, "PEMANFAATAN TEKNOLOGI INTERNET OF THINGS (IOT) PADA BIDANG PERTANIAN," *Jurnal Mahasiswa Teknik Informatika (JATI)*, vol. 7, no. 1, pp. 1–5, 2023.

[27] M. A. J. Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, "IoT Architecture," in *Towards the Internet of Things Architectures, Security, and Applications*, EAI/Springer Innovations in Communication and Computing, 2020, ch. 2, pp. 9–31. doi: 10.1007/978-3-030-18468-1_2.

[28] S. A. Al-Qaseemi, M. F. Almuhim, H. A. Almuhim, and S. R. Chaudhry, "IoT Architecture Challenges and Issues: Lack of Standardization," in *Future Technologies Conference (FTC)*, San Fransisco: IEEE, Dec. 2016, pp. 731–738. doi: https://doi.org/10.1109/FTC.2016.7821686.

[29] K. Chen *et al.*, "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," *Journal of Hardware and Systems Security*, vol. 2, no. 2, pp. 97–110, Jun. 2018, doi: 10.1007/s41635-017-0029-7.

[30] A. Lohachab and B. Karambir, "Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks," *Journal of Communications and Information Networks*, vol. 3, no. 3, pp. 57–78, Sep. 2018, doi: 10.1007/s41650-018-0022-5.

[31] A. Munshi, N. A. Alqarni, and N. A. Almalki, "DDoS Attack on IoT Devices," in *3rd International Conference on Computer Applications & Information Security (ICCAIS)*, IEEE, 2020. doi: https://doi.org/10.1109/ICCAIS48893.2020.9096818.

[32] J. C. J. Sihombing, D. P. Kartikasari, and A. Bhawiyuga, "Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software-Defined Network (SDN)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 10, pp. 9608–9613, 2019, [Online]. Available: http://j-ptiik.ub.ac.id

[33] G. Ramadhan, Y. Kurniawan, and C. S. Kim, "Design of TCP SYN Flood DDoS Attack Detection Using Artificial Immune Systems," in *IEEE 6th International Conference on System Engineering and Technology (ICSET)*, Bandung: IEEE, Oct. 2016. doi: https://doi.org/10.1109/ICSEngT.2016.7849626.

[34] D. Stiawan *et al.*, "Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network," *IEEE Access*, vol. 9, pp. 116475–116484, 2021, doi: 10.1109/ACCESS.2021.3105517.

[35] V. K. Yadav, M. C. Trivedi, and B. M. Mehtre, "DDA: An Approach to Handle DDoS (Ping Flood) Attack," in *Proceedings of International Conference on ICT for Sustainable Development*, Springer Verlag, 2016, pp. 11–23. doi: 10.1007/978-981-10-0129-1_2.

[36] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” *Cybersecurity*, vol. 2, no. 1, pp. 1–22, Dec. 2019, doi: 10.1186/s42400-019-0038-7.

[37] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, “Evaluation of Machine Learning Algorithms for Intrusion Detection System,” in *IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, 2017, pp. 277–282. doi: https://doi.org/10.1109/SISY.2017.8080566.

[38] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan, “Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review,” in *Third International Conference on Computing and Network Communications (CoCoNet’19)*, Elsevier B.V., 2020, pp. 1251–1260. doi: 10.1016/j.procs.2020.04.133.

[39] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, “Intrusion detection systems for IoT-based smart environments: a survey,” *Journal of Cloud Computing*, vol. 7, no. 1, pp. 1–20, Dec. 2018, doi: 10.1186/s13677-018-0123-6.

[40] M. A. Alsoufi *et al.*, “Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review,” *Applied Sciences*, vol. 11, no. 18, Sep. 2021, doi: 10.3390/app11188383.

[41] Dr. S. Smys, Dr. Abul Basar, and Dr. Haoxiang Wang, “Hybrid Intrusion Detection System for Internet of Things (IoT),” *Journal of ISMAC*, vol. 2, no. 4, pp. 190–199, Sep. 2020, doi: 10.36548/jismac.2020.4.002.

[42] Q. Niyaz, W. Sun, A. Y. Javaid, and M. Alam, “A Deep Learning Approach for Network Intrusion Detection System,” in *EAI International Conference on Bio-inspired Information and Communications Technologies (BICT)*, 2015. doi: 10.4108/eai.3-12-2015.2262516.

[43] Z. Mahdi, N. Abdalhussien, N. Mahmood, and R. Zaki, “Detection of Real-Time Distributed Denial-of-Service (DDoS) Attacks on Internet of Things (IoT) Networks Using Machine Learning Algorithms,” *Computers, Materials and Continua*, vol. 80, no. 2, pp. 2139–2159, 2024, doi: 10.32604/cmc.2024.053542.

[44] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, pp. 1–29, Jan. 2021, doi: 10.1002/ett.4150.

[45] P. Papadopoulos, O. Thornewill von Essen, N. Pitropakis, C. Chrysoulas, A. Mylonas, and W. J. Buchanan, “Launching Adversarial Attacks against Network Intrusion Detection Systems for IoT,” *Journal of Cybersecurity and Privacy*, vol. 1, no. 2, pp. 252–273, Jun. 2021, doi: 10.3390/jcp1020014.

[46] R. Saravanan and P. Sujatha, “A State of Art Techniques on Machine Learning Algorithms: A Perspective of Supervised Learning Approaches in Data Classification,” in *Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, [IEEE], 2018, pp. 945–949. doi: https://doi.org/10.1109/ICCONS.2018.8663155.

[47] B. Mahesh, “Machine Learning Algorithms - A Review,” *International Journal of Science and Research (IJSR)*, vol. 9, no. 1, pp. 381–386, Jan. 2020, doi: 10.21275/art20203995.

[48] O. F.Y, A. J.E.T, A. O, H. J. O, O. O, and A. J, "Supervised Machine Learning Algorithms: Classification and Comparison," *International Journal of Computer Trends and Technology (IJCTI)*, vol. 48, no. 3, pp. 128–138, Jun. 2017, doi: 10.14445/22312803/IJCTT-V48P126.

[49] Q. Bi, K. E. Goodman, J. Kaminsky, and J. Lessler, "What is Machine Learning? A Primer for the Epidemiologist," *Am J Epidemiol*, vol. 188, no. 12, pp. 2222–2239, Dec. 2019, doi: 10.1093/aje/kwz189.

[50] V. Nasteski, "An overview of the supervised machine learning methods," *HORIZONS B*, vol. 4, pp. 51–62, Dec. 2017, doi: 10.20544/horizons.b.04.1.17.p05.

[51] O. F. Y, A. J. E. T, H. J. O, O. O, and A. J, "Supervised Machine Learning Algorithms: Classification and Comparison," *International Journal of Computer Trends and Technology (IJCTI)*, vol. 48, no. 3, pp. 128–138, 2017, doi: 10.14445/22312803/IJCTT-V48P126.

[52] M. W. Berry, A. Mohamed, and B. W. Yap, *Supervised and Unsupervised Learning for Data Science*. doi: https://doi.org/10.1007/978-3-030-22475-2.

[53] I. Muhammad and Z. Yan, "SUPERVISED MACHINE LEARNING APPROACHES: A SURVEY," *ICTACT Journal on Soft Computing*, vol. 05, no. 03, pp. 946–952, Apr. 2015, doi: 10.21917/ijsc.2015.0133.

[54] S. Naeem, A. Ali, S. Anam, and M. M. Ahmed, "An Unsupervised Machine Learning Algorithms: Comprehensive Review," *International Journal of Computing and Digital Systems*, vol. 13, no. 1, pp. 911–921, 2023, doi: 10.12785/ijcds/130172.

[55] J. Andreanus, A. Kurniawan, and S. Panas, "Sejarah, Teori Dasar dan Penerapan Reinforcement Learning: Sebuah Tinjauan Pustaka," *Jurnal Telematika*, vol. 12, no. 2, pp. 113–118, 2017, doi: https://doi.org/10.61769/telematika.v12i2.193.

[56] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method," *Symmetry (Basel)*, vol. 14, no. 6, pp. 1–15, Jun. 2022, doi: 10.3390/sym14061095.

[57] A. Parmar, R. Katariya, and V. Patel, "A Review on Random Forest: An Ensemble Classifier," in *International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018*, vol. 26, Springer Science and Business Media Deutschland GmbH, 2019, pp. 758–763. doi: 10.1007/978-3-030-03146-6_86.

[58] R. T. Yunardi and N. Z. Dina, "IMPLEMENTASI DECISION TREE, RANDOM FOREST, DAN ADABOOST UNTUK KLASIFIKASI VARIETAS BIJI GANDUM," in *DATA MINING dan MACHINE LEARNING dengan Orange3 Tutorial dan Aplikasinya*, A. Abadi, Ed., Surabaya: Airlangga University Press, 2022, ch. 6. Accessed: Nov. 07, 2024. [Online]. Available: https://books.google.co.id/books?id=hplvEAAAQBAJ&pg=PA77&source=gbs_toc_r&cad=2#v=onepage&q&f=false

[59] C. Aroef, Y. Rivan, and Z. Rustam, "Comparing random forest and support vector machines for breast cancer classification," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 18, no. 2, pp. 815–821, Apr. 2020, doi: 10.12928/TELKOMNIKA.V18I2.14785.

[60] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques," in *Amity International Conference on Artificial Intelligence (AICAI)*, Institute of Electrical and Electronics Engineers, 2019, pp. 870–875. doi: https://doi.org/10.1109/AICAI.2019.8701238.

[61] S. E. Prasetyo, P. H. Prastyo, and S. Arti, "A Cardiotocographic Classification using Feature Selection: A comparative Study," *JITCE (Journal of Information Technology and Computer Engineering)*, vol. 5, no. 01, pp. 25–32, Mar. 2021, doi: 10.25077/jitce.5.01.25-32.2021.

[62] K. Reddy Madhavi, M. N. Mohd Nawi, B. Bhaskar Reddy, K. Baboji, K. Hari Kishore, and S. V. Manikanthan, "Energy efficient target tracking in wireless sensor network using PF-SVM (particle filter-support vector machine) technique," *Sensors*, vol. 26, Apr. 2023, doi: 10.1016/j.measen.2023.100667.

[63] J. Cai, J. Luo, S. Wang, and S. Yang, "Feature selection in machine learning: A new perspective," *Neurocomputing*, vol. 300, pp. 70–79, Jul. 2018, doi: 10.1016/j.neucom.2017.11.077.

[64] K. Kurniabudi, E. A. Winanto, L. Y. Astri, and S. Sharipuddin, "Ensemble Method for Anomaly Detection On the Internet of Things," *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, vol. 18, no. 1, p. 25, Jan. 2024, doi: 10.22146/ijccs.85834.

[65] R. Panthong and A. Srivihok, "Wrapper Feature Subset Selection for Dimension Reduction Based on Ensemble Learning Algorithm," in *Procedia Computer Science*, Elsevier, 2015, pp. 162–169. doi: 10.1016/j.procs.2015.12.117.

[66] F. Kamalov, S. Elnaffarr, A. Cherukuri, and A. Jonnalagadda, "Forward feature selection: empirical analysis," *Journal of Intelligent Systems and Internet of Things*, vol. 11, no. 1, pp. 44–54, 2024, doi: 10.54216/JISIoT.110105.

[67] A. Vabalas, E. Gowen, E. Poliakoff, and A. J. Casson, "Machine learning algorithm validation with a limited sample size," *PLoS One*, vol. 14, no. 11, pp. 1–20, Nov. 2019, doi: 10.1371/journal.pone.0224365.

[68] L. Mardiana, D. Kusnandar, and N. Satyahadewi, "ANALISIS DISKRIMINAN DENGAN K FOLD CROSS VALIDATION UNTUK KLASIFIKASI KUALITAS AIR DI KOTA PONTIANAK," *Buletin Ilmiah Mat. Stat. dan Terapannya (Bimaster)*, vol. 11, no. 1, pp. 97–102, 2022, doi: https://doi.org/10.26418/bbimst.v11i1.51608.

[69] R. R. Adhitya, Wina Witanti, and Rezki Yuniarti, "PERBANDINGAN METODE CART DAN NAÏVE BAYES UNTUK KLASIFIKASI CUSTOMER CHURN," *INFOTECH journal*, vol. 9, no. 2, pp. 307–318, Jul. 2023, doi: 10.31949/infotech.v9i2.5641.

[70] D. Normawati and S. A. Prayogi, "Implementasi Naïve Bayes Classifier Dan Confusion Matrix Pada Analisis Sentimen Berbasis Teks Pada Twitter," *Jurnal Sains Komputer & Informatika (J-SAKTI)*, vol. 5, no. 2, pp. 697–711, 2021, doi: http://dx.doi.org/10.30645/j-sakti.v5i2.369.

[71] D. A. Senthilselvi, D. B. J. Chelliah, and M. S. S. Pandi, *Machine Learning*, I. Shanlax Publications, 2021. Accessed: Nov. 15, 2024. [Online]. Available: https://books.google.co.id/books?id=vUpgEAAAQBAJ&printsec=copyright&hl=id#v=onepage&q&f=false

[72] A. C. Müller and S. Guido, *Introduction to Machine Learning with Python A Guide for Data Scientists*. O'Reilly Media , 2017.

[73] P. Gupta and N. K. Sehgal, *Introduction to Machine Learning in the Cloud with Python: Concepts and Practices*. Springer International Publishing, 2021. doi: 10.1007/978-3-030-71270-9.

[74] S. M. Tseng, Y. Q. Wang, and Y. C. Wang, "Multi-Class Intrusion Detection Based on Transformer for IoT Networks Using CIC-IoT-2023 Dataset," *Future Internet*, vol. 16, no. 8, pp. 1–25, Aug. 2024, doi: 10.3390/fi16080284.

[75] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, pp. 1–26, Jul. 2023, doi: 10.3390/s23135941.

[76] S. Al Emadi, A. Al Mohannadi, and F. Al Senaid, "Using Deep Learning Techniques for Network Intrusion Detection," in *IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, IEEE, 2020, pp. 171–176. doi: https://doi.org/10.1109/ICIoT48696.2020.9089524.

[77] E. A. Winanto, Y. Novianto, S. Sharipuddin, I. S. Wijaya, and P. A. Jusia, "PENINGKATAN PERFORMA DETEKSI SERANGAN MENGGUNAKAN METODE PCA DAN RANDOM FOREST," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 2, pp. 285–290, Apr. 2024, doi: 10.25126/jtiik.20241127678.

[78] N. Meti, N. D. G, and V. P. Baligar, "Detection of Distributed Denial of Service Attacks using Machine Learning Algorithms in Software Defined Networks," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, IEEE, 2017, pp. 1–6. doi: https://doi.org/10.1109/ICACCI.2017.8126031.

[79] D. Alghazzawi, O. Bamasaq, H. Ullah, and M. Z. Asghar, "Efficient Detection of DDoS Attacks Using a Hybrid Deep Learning Model with Improved Feature Selection," *Applied Sciences (Switzerland)*, vol. 11, no. 24, pp. 1–22, Dec. 2021, doi: 10.3390/app112411634.