DAFTAR PUSTAKA

[1] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), "Buletin APJII, Edisi 84: Membangun Kembali Impian Indonesia Jadi Hub Internet Dunia," Apr. 2021. [Online]. Available: https://apjii.or.id/assets/media/buletin_apjii_edisi_84_-_april_2021_bulletin.pdf

[2] CSIRT–BSSN, "Lanskap Keamanan Siber Indonesia 2023," Feb. 2025. [Online]. Available: https://csirt.kemenpora.go.id/wp-content/uploads/2025/02/keamanan.pdf

[3] K. Al Jallad, M. Aljnidi, and M. ~S. Desouki, "Anomaly detection optimization using big data and deep learning to reduce false-positive," *J Big Data*, vol. 7, no. 68, pp. 1–16, 2022, [Online]. Available: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-022-00616-0

[4] Z. Iqbal, A. Sajid, M. N. Zakki, A. Zafar, and A. Mehmood, "Role of Machine and Deep Learning Algorithms in Secure Intrusion Detection Systems (IDS) for IOT & Smart Cities," *International Journal of Information Technology, Research and Applications*, vol. 3, no. 4, pp. 1–16, Nov. 2024, doi: 10.59461/ijitra.v3i4.111.

[5] P. H K, P. Kumar, , Pradeepa A J, P. S, and S. F. Khan, "Detection Of DDOS Attack Using Machine Learning," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, vol. 09, no. 01, pp. 1–9, Jan. 2025, doi: 10.55041/IJSREM40595.

[6] A. ARQANE, O. Boutkhoum, H. Boukhriss, and A. El Moutaouakkil, "Intrusion Detection System using Ensemble Learning Approaches: A Systematic Literature Review," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 13, pp. 160–175, Oct. 2022, doi: 10.3991/ijoe.v18i13.33519.

[7] Mahesh T R, V Vivek, and Vinoth Kumar, "Implementation of Machine Learning-Based Data Mining Techniques for IDS," *International Journal of Information Technology, Research and Applications*, vol. 2, no. 1, pp. 7–13, Mar. 2023, doi: 10.59461/ijitra.v2i1.23.

[8] A. Hamarshe, H. I. Ashqar, and M. Hamarsheh, "Detection of DDoS Attacks in Software Defined Networking Using Machine Learning Models," Mar. 2023.

[9] K. Kaur, "A Study of Cyber Security and Cyber Threats," *CGC International Journal of Contemporary Technology and Research*, vol. 3, no. 1, pp. 154–157, Dec. 2020, doi: 10.46860/cgcijctr.2020.12.26.154.

[10] K. Gusnanda, N. Ulfadillah, and T. Sumarni, "STRUKTUR BASIS DATA DI ERA DIGITAL (IMPLEMENTASI PENGAMANAN BASIS DATA DI ERA GLOBAL)," *Kohesi: Jurnal Sains dan Teknologi*, vol. 3, no. 6, pp. 22–32, 2024.

[11] F. Pujiani and R. Bisma, "Strategi Optimalisasi Manajemen Konfigurasi untuk Keamanan Informasi Berdasarkan ISO/IEC 27001: 2022," *Journal of Emerging Information System and Business Intelligence (JEISBI)*, vol. 5, no. 3, pp. 223–228, 2024.

[12] L. Caviglione *et al.*, "Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection," *IEEE Access*, vol. 9, pp. 5371–5396, 2021, doi: 10.1109/ACCESS.2020.3048319.

[13] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterp Inf Syst*, vol. 16, no. 4, pp. 527–565, Apr. 2022, doi: 10.1080/17517575.2021.1896786.

[14] L. F. Eliyan and R. Di Pietro, "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges," *Future Generation Computer Systems*, vol. 122, pp. 149–171, Sep. 2021, doi: 10.1016/j.future.2021.03.011.

[15] B. I. Bakare and S. M. Ekolama, "Preventing Man-in-The-Middle (MiTM) Attack of GSM Calls," *European Journal of Electrical Engineering and Computer Science*, vol. 5, no. 4, pp. 63–68, Aug. 2021, doi: 10.24018/ejece.2021.5.4.336.

[16] P. Tang, W. Qiu, Z. Huang, H. Lian, and G. Liu, "Detection of SQL injection based on artificial neural network," *Knowl Based Syst*, vol. 190, p. 105528, Feb. 2020, doi: 10.1016/j.knosys.2020.105528.

[17] M. NIKLEKAJ, "Security in Computer Networks: Threats, Challenges, and Protection," *Ingenious*, vol. 3, no. 1, pp. 51–60, 2023, doi: 10.58944/mcne2043.

[18] A. D. Lazarov, "Mathematical Modelling of Malware Intrusion in Computer Networks," *Cybernetics and Information Technologies*, vol. 22, no. 3, pp. 29–47, Sep. 2022, doi: 10.2478/cait-2022-0026.

[19] N. Gulia, K. Solanki, and S. Dalal, "Comparative Analysis to Identify the Effective Machine Learning Method for Prediction of DDOS Attack," in *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, IEEE, Oct. 2022, pp. 1–5. doi: 10.1109/ICRITO56286.2022.9965126.

[20] N. Polakovicova, A. V. Adji, L. J. Myhill, and A. R. Williams, "Whipworm Infection in Mice Increases Coinfection of Enteric Pathogens but Promotes Clearance of *Ascaris* Larvae From the Lungs," *J Infect Dis*, vol. 227, no. 12, pp. 1428–1432, Jun. 2023, doi: 10.1093/infdis/jiad063.

[21] C. M. Mwange and E. C. Cankaya, "Android Trojan Horse Spyware Attack: A Practical Implementation," in *2024 12th International Symposium on Digital*

Forensics and Security (ISDFS), IEEE, Apr. 2024, pp. 1–5. doi: 10.1109/ISDFS60797.2024.10527296.

[22] M. Aljabri *et al.*, "Ransomware detection based on machine learning using memory features," *Egyptian Informatics Journal*, vol. 25, p. 100445, Mar. 2024, doi: 10.1016/j.eij.2024.100445.

[23] Dr. S. Kumar and R. K. Dubey, "SPYWARE AS BARRIER TO E-MARKETING: AN EMPIRICAL STUDY," *Proceeding of International Conference on Science, Health, And Technology*, pp. 49–64, Sep. 2023, doi: 10.47701/icohetech.v4i1.3372.

[24] A. Muftiadi, T. P. M. Agustina, and M. Evi, "Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking," *Hexatech: Jurnal Ilmiah Teknik*, vol. 1, no. 2, pp. 60–65, 2022.

[25] J. Jessima, E. Ginting, P. Sahara, and S. N. Tambunan, "Ancaman denial of service attack dalam eksploitasi keamanan sistem informasi," *Unes Journal of Information System*, vol. 8, no. 1, pp. 9–19, 2023.

[26] S. Gunawan, A. A. R. Santosa, and E. M. S. Sakti, "Analisis Keamanan Jaringan 5G: Ancaman dan Upaya Mitigasi," *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, vol. 25, no. 2, pp. 54–62, 2024.

[27] A. Bastian, H. Sujadi, and L. Abror, "Analisis keamanan aplikasi data pokok pendidikan (DAPODIK) menggunakan penetration testing dan SQL injection," *INFOTECH journal*, vol. 6, no. 2, pp. 65–70, 2020.

[28] A. Bastian, H. Sujadi, and L. Abror, "Analisis keamanan aplikasi data pokok pendidikan (DAPODIK) menggunakan penetration testing dan SQL injection," *INFOTECH journal*, vol. 6, no. 2, pp. 65–70, 2020.

[29] Z. I. Sumayyah, S. D. S. Permana, M. Tsabit, and A. Setiawan, "Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDos) terhadap Website Ilegal dengan Kali Linux," *Journal of Internet and Software Engineering*, vol. 1, no. 2, p. 14, 2024.

[30] A. Malhotra, I. E. Cohen, E. Brakke, and S. Goldberg, "Attacking the Network Time Protocol," in *Proceedings 2016 Network and Distributed System Security Symposium*, Reston, VA: Internet Society, 2016. doi: 10.14722/ndss.2016.23090.

[31] M. F. Saiyed and I. Al-Anbagi, "Flow and unified information-based DDoS attack detection system for multi-topology IoT networks," *Internet of Things*, vol. 24, p. 100976, Dec. 2023, doi: 10.1016/j.iot.2023.100976.

[32] K. Singh, P. Singh, and K. Kumar, "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges," *Comput Secur*, vol. 65, pp. 344–372, Mar. 2017, doi: 10.1016/j.cose.2016.10.005.

[33] A. Aguru and S. Erukala, "OTI-IoT: A Blockchain-based Operational Threat Intelligence Framework for Multi-vector DDoS Attacks," *ACM Trans Internet Technol*, vol. 24, no. 3, pp. 1–31, Aug. 2024, doi: 10.1145/3664287.

[34] H. Mateen and M. Shahzad, “Factors Effecting Businesses due to Distributed Denial of Service (DDoS) Attack,” in *2021 International Conference on Innovative Computing (ICIC)*, IEEE, Nov. 2021, pp. 1–7. doi: 10.1109/ICIC53490.2021.9692965.

[35] I. M. Razzanda and M. Koprawi, “Implementasi IDS dan IPS terhadap Serangan TCP Port Scanning dan ICMP Flooding,” *The Indonesian Journal of Computer Science*, vol. 13, no. 4, 2024.

[36] Prof. D. Mane, “Machine Learning Algorithms for Intrusion Detection in Cybersecurity,” *Int J Res Appl Sci Eng Technol*, vol. 11, no. 5, pp. 6315–6321, May 2023, doi: 10.22214/ijraset.2023.52788.

[37] A. Pal Singh and M. Deep Singh, “Analysis of Host-Based and Network-Based Intrusion Detection System,” *International Journal of Computer Network and Information Security*, vol. 6, no. 8, pp. 41–47, Jul. 2014, doi: 10.5815/ijcnis.2014.08.06.

[38] I. P. Saputra, E. Utami, and A. H. Muhammad, “Comparison of Anomaly Based and Signature Based Methods in Detection of Scanning Vulnerability,” in *2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, IEEE, Oct. 2022, pp. 221–225. doi: 10.23919/EECSI56542.2022.9946485.

[39] C. Ieracitano, A. Adeel, F. C. Morabito, and A. Hussain, “A novel statistical analysis and autoencoder driven intelligent intrusion detection approach,” *Neurocomputing*, vol. 387, pp. 51–62, Apr. 2020, doi: 10.1016/j.neucom.2019.11.016.

[40] P. Perrone, F. Flammini, and R. Setola, “Machine Learning for Threat Recognition in Critical Cyber-Physical Systems,” in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, IEEE, Jul. 2021, pp. 298–303. doi: 10.1109/CSR51186.2021.9527979.

[41] C. Majdoubi, S. El mendili, and Y. Gahi, “Data Security Patterns for Critical Big Data Systems,” in *2023 IEEE 6th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*, IEEE, Nov. 2023, pp. 01–08. doi: 10.1109/CloudTech58737.2023.10366149.

[42] H. Lu, B. Ying, X. Che, Z. Jin, M. Wang, and S. Wu, “DDoS attack detection method based on One-Hot coding and improved ResNet18,” in *2023 4th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*, IEEE, Jun. 2023, pp. 196–199. doi: 10.1109/AINIT59027.2023.10210725.

[43] J. Zhao, Y. Liu, Q. Zhang, and X. Zheng, “CNN-AttBiLSTM Mechanism: A DDoS Attack Detection Method Based on Attention Mechanism and CNN-BiLSTM,” *IEEE Access*, vol. 11, pp. 136308–136317, 2023, doi: 10.1109/ACCESS.2023.3334916.

[44] T. Tu, “DDoS Analysis and Detection with Machine Learning Algorithms,” *Scholarly Review Journal*, vol. Fall 2023, no. 6, Sep. 2023, doi: 10.70121/001c.121699.

[45] M. Alfathe, Aida Mustapha, Huthaifa L. Mohamed, Salama A Mostafa, Yousif Khalid Yousif, and Ali H. Al-Shakarchi, “Detecting DDoS Attacks in Network Traffic Based on Supervised Machine Learning Techniques,” *Al-Noor Journal for Information Technology and Cybersecurity*, vol. 1, Dec. 2024, doi: 10.69513/jnfit.v1.i0.a2.

[46] S. S and S. S, “DDOS Detection Using ML and Deep Learning Approaches,” in *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*, IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/CSITSS64042.2024.10817014.

[47] Y. Wu, “DDos attack detection method based on machine learning,” *Applied and Computational Engineering*, vol. 18, no. 1, pp. 88–95, Oct. 2023, doi: 10.54254/2755-2721/18/20230968.

[48] Sutrisno, U. Rahardja, S. Wijono, T. Wahyono, I. Sembiring, and I. R. Widiasari, “Effective DDoS Detection through Innovative Algorithmic Approaches in Machine Learning,” in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*, IEEE, Aug. 2024, pp. 1–7. doi: 10.1109/ICCIT62134.2024.10701265.

[49] R. A. M. Rudro, MD. F. A. AL SOHAN, S. K. Chaity, and R. I. Reya, “Enhancing DDoS Attack Detection Using Machine Learning: A Framework with Feature Selection and Comparative Analysis of Algorithms,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 14, no. 03, pp. 1185–1192, Nov. 2023, doi: 10.61841/turcomat.v14i03.14086.

[50] S. Ahmadi, “AI in the Detection and Prevention of Distributed Denial of Service (DDoS) Attacks,” *SSRN Electronic Journal*, 2025, doi: 10.2139/ssrn.5011038.