DAFTAR PUSTAKA

[1] K. Nosalska and G. Mazurek, “Marketing principles for Industry 4.0 - a conceptual framework,” *Eng. Manag. Prod. Serv.*, vol. 11, no. 3, pp. 9–20, 2019, doi: 10.2478/emj-2019-0016.

[2] Badan Siber dan Sandi Negara, “Laporan Tahunan Monitoring Keamanan Siber 2021,” 2022, pp. 54–55. [Online]. Available: https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw

[3] X. Chen, *Distributed denial of service attack and defense*, vol. 3. 2010. doi: 10.1109/ICEIT.2010.5608362.

[4] Amarudin, R. Ferdiana, and Widyawan, “A Systematic Literature Review of Intrusion Detection System for Network Security: Research Trends, Datasets and Methods,” *ICICoS 2020 - Proceeding 4th Int. Conf. Informatics Comput. Sci.*, pp. 0–5, 2020, doi: 10.1109/ICICoS51170.2020.9299068.

[5] E. Osterweil, A. Stavrou, and L. Zhang, “20 Years of DDoS: a Call to Action,” vol. 1, no. 1, pp. 1–11, 2019, [Online]. Available: http://arxiv.org/abs/1904.02739

[6] M. Zamani, “Machine learning techniques for intrusion detection,” *Handb. Res. Intrusion Detect. Syst.*, no. December 2013, pp. 47–65, 2020, doi: 10.4018/978-1-7998-2242-4.ch003.

[7] B. Purnama, *Pengantar Machine Learning*. 2019. [Online]. Available: https://aptika.kominfo.go.id/wp-content/uploads/2018/12/Kajian-Kominfo-CIPG-compressed.pdf

[8] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, “Analysis and Detection of DDoS on Cloud Computing Environment using Machine Learning Techniques,” *Commun. Comput. Inf. Sci.*, vol. 1076, pp. 260–273, 2019, doi: 10.1007/978-981-15-0111-1_24.

[9] Y. Chen, J. Hou, Q. Li, and H. Long, “DDoS attack detection based on random forest,” *Proc. 2020 IEEE Int. Conf. Prog. Informatics Comput. PIC 2020*, pp. 328–334, 2020, doi: 10.1109/PIC50277.2020.9350788.

[10] 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, 2022, doi: 10.3390/sym14061095.

[11] V. Gaur and R. Kumar, “Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices,” *Arab. J. Sci. Eng.*, vol. 47, no. 2, pp. 1353–1374, 2022, doi: 10.1007/s13369-021-05947-3.

[12] A. M. Makkawi and A. Yousif, “Machine Learning for Cloud DDoS Attack Detection: A Systematic Review,” *Proc. 2020 Int. Conf. Comput. Control. Electr. Electron. Eng. ICCCEEE 2020*, 2021, doi: 10.1109/ICCCEEE49695.2021.9429678.

[13] C. D. Sutton, *Classification and Regression Trees, Bagging, and Boosting*, vol. 24, no. 04. Elsevier Masson SAS, 2005. doi: 10.1016/S0169-7161(04)24011-1.

[14] I. M. Wasanta, I. P. Gede, H. Suputra, I. M. Widiartha, and I. G. A. Gede, “Klasifikasi Serangan Distributed Denial of Service (DDoS) Menggunakan Random Forest dengan CFS,” vol. 11, no. 2, pp. 215–222, 2022.

[15] Notohadiprawiro, T. (2006). Metode penelitian dan penulisan ilmiah. *Dalam Jurnal Repro, ilmu Tanah Universitas Gadjah Mada*.

[16] Murad, D. F. (2020). Systematic literature review (slr) approach.

[17] Mishra, S., Sharma, S. K., & Alowaidi, M. A. (2021). *Analysis of security issues of cloud-based web applications. Journal of Ambient Intelligence and Humanized Computing*, 12(7), 7051-7062.

[18] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California law review*, 817-885.

[19] Gupta, B. B. (2011). *An Introduction to DDoS Attacks and Defense Mechanisms: An Analyst's Handbook*. Lap Lambert Academic Pub.

[20] Radivojac, P., & White, M. (2019). Machine learning handbook.

[21] Hassanien, A. E., & Gaber, T. (Eds.). (2017). *Handbook of research on machine learning innovations and trends*. IGI global.

[22] Ye, N. (Ed.). (2003). *The handbook of data mining*. CRC Press.

[23] Maimon, O., & Rokach, L. (Eds.). (2005). Data mining and knowledge discovery handbook.

[24] Strobl, C., Malley, J., & Tutz, G. (2009). An introduction to recursive partitioning: rationale, application, and characteristics of classification and regression trees, bagging, and random forests. *Psychological methods*, *14*(4), 323.

[25] Satmoko, D. B., Sukarno, P., & Jadied, E. M. (2018). Peningkatan Akurasi Pendeteksian Serangan DDoS Menggunakan Multiclassifier Ensemble Learning dan Chi-Square. vol, 5, 7977-7985.

[26] Dietterich, T. G. (2002). Ensemble learning. *The handbook of brain theory and neural networks*, *2*(1), 110-125.

[27] Breiman, L. (1996). Bagging predictors. *Machine learning*, *24*, 123-140.

[28] Yanti, H. A., Sukoco, H., & Neyman, S. N. (2021). Pemodelan Identifikasi Trafik Bittorrent Dengan Pendekatan Correlation Based Feature Selection (CFS) Menggunakan Algoritme Decision Tree (C4. 5). *CESS (Journal of Computer Engineering, System and Science)*, *6*(1), 1-9.

[29] VanderPlas, J. (2016). *Python data science handbook: Essential tools for working with data*. " O'Reilly Media, Inc.".

[30] Bernard, J. (2016). *Python Recipes Handbook: A Problem-Solution Approach*. Apress.

[31] Pech, V., Shatalin, A., & Voelter, M. (2013, September). JetBrains MPS as a tool for extending Java. In *Proceedings of the 2013 International Conference on Principles and Practices of Programming on the Java Platform: Virtual Machines, Languages, and Tools* (pp. 165-168).