DAFTAR PUSTAKA

[1] Statista, "Internet and social media users in the world 2023 | Statista," 2023. https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed Jan. 03, 2023).

[2] D. K. Bhattacharyya and J. K. Kalita, *Network Anomaly Detection: ML Perspective*. 2014.

[3] V. Ambalavanan and Shanthi Bala P., "Cyber Threats Detection and Mitigation Using Machine Learning," pp. 132–149, 2019, doi: 10.4018/978-1-5225-9611-0.ch007.

[4] F. Farahmand, S. B. Navathe, P. H. Enslow, and G. P. Sharp, "Managing vulnerabilities of information systems to security incidents," *ACM Int. Conf. Proceeding Ser.*, vol. 50, pp. 348–354, 2003, doi: 10.1145/948005.948050.

[5] National Cyber and Crypto Agency, "Yearly Report Cyber Security 2021," pp. 16–218, 2022, [Online]. Available: https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw

[6] H. Teymourlouei, "Preventative Measures in Cyber & Ransomware Attacks for Home & Small Businesses' Data - ProQuest," *Proc. Int. Conf. Sci. Comput. (CSC); Athens*, no. April, pp. 87–93, 2018, [Online]. Available: https://www.proquest.com/docview/2140020824/abstract/EB63997AD03044E7PQ/28?accountid=14516

[7] O. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8, pp. 6249–6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

[8] M. Christen, B. Gordijn, and M. Loi, *The Ethics of Cybersecurity*. 2022. doi: 10.21428/cb6ab371.d27262ff.

[9] "Cybercriminals attack users with 400,000 new malicious files daily – that is 5% more than in 2021 | Kaspersky." https://www.kaspersky.com/about/press-releases/2022_cybercriminals-attack-users-with-400000-new-malicious-files-daily---that-is-5-more-than-in-2021 (accessed Jan. 02, 2023).

[10] L. Li *et al.*, “On Locating Malicious Code in Piggybacked Android Apps,” *J. Comput. Sci. Technol.*, vol. 32, no. 6, pp. 1108–1124, 2017, doi: 10.1007/s11390-017-1786-z.

[11] A. Kamboj, P. Kumar, A. K. Bairwa, and S. Joshi, “Detection of malware in downloaded files using various machine learning models,” *Egypt. Informatics J.*, vol. 24, no. 1, pp. 81–94, 2023, doi: 10.1016/j.eij.2022.12.002.

[12] D. Gibert, C. Mateu, and J. Planes, “The rise of machine learning for detection and classification of malware: Research developments, trends and challenges,” *J. Netw. Comput. Appl.*, vol. 153, no. November 2019, p. 102526, 2020, doi: 10.1016/j.jnca.2019.102526.

[13] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, “Robust Intelligent Malware Detection Using Deep Learning,” *IEEE Access*, vol. 7, no. c, pp. 46717–46738, 2019, doi: 10.1109/ACCESS.2019.2906934.

[14] D. Wang, P. Cui, and W. Zhu, “Structural deep network embedding,” *Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min.*, vol. 13-17-Augu, pp. 1225–1234, 2016, doi: 10.1145/2939672.2939753.

[15] J. Saxe and K. Berlin, “Deep Neural Network Based Malware Detection Using Two Dimensional Binary Program Features,” *Proc. 2015 10th Int. Conf. Malicious Unwanted Softw.*, 2016.

[16] A. Makandar and A. Patrot, “Malware analysis and classification using Artificial Neural Network,” *Int. Conf. Trends Autom. Commun. Comput. Technol. I-TACT 2015*, 2016, doi: 10.1109/ITACT.2015.7492653.

[17] B. B. Rad, M. K. H. Nejad, and M. Shahpasand, “Malware classification and detection using artificial neural network,” *J. Eng. Sci. Technol.*, vol. 13, no. Special Issue on ICCSIT 2018, pp. 14–23, 2018.

[18] A. A. Ahmed, W. A. Jabbar, A. S. Sadiq, and H. Patel, “Deep Learning-Based Classification Model for Botnet Attack Detection,” *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 7, pp. 3457–3466, 2022, doi: 10.1007/S12652-020-01848-9/METRICS.

[19] N. Salleh, “Introduction to systematic literature review.” pp. 1–33, 2014.

[Online]. Available: https://cgspace.cgiar.org/handle/10568/108373

[20] R. Kumar, *Research Methodology: A Step-by-Step Guide for Beginners*, Third Edit. London: SAGE Publications Ltd, 2010.

[21] R. S. Wahono, “Research Methodology: Literature Review.” [Online]. Available: https://slideplayer.info/slide/5252670/

[22] F. Al Huda, W. F. Mahmudy, and H. Tolle, “Android malware detection using backpropagation neural network,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 4, no. 1, pp. 240–244, 2016, doi: 10.11591/ijeecs.v4.i1.pp240-244.

[23] Z.-P. Pan, C. Feng, and C.-J. Tang, “Malware Classification Based on the Behavior Analysis and Back Propagation Neural Network,” *ITM Web Conf.*, vol. 7, p. 02001, 2016, doi: 10.1051/itmconf/20160702001.

[24] E. Raff, J. Barker, J. Sylvester, R. Brandon, B. Catanzaro, and C. Nicholas, “Malware Detection by Eating a Whole EXE,” pp. 268–276, 2017, [Online]. Available: http://arxiv.org/abs/1710.09435

[25] Y. Ki, E. Kim, and H. K. Kim, “A novel approach to detect malware based on API call sequence analysis,” *Int. J. Distrib. Sens. Networks*, vol. 2015, 2015, doi: 10.1155/2015/659101.

[26] D. Hindarto, “Perbandingan Kinerja Akurasi Klasifikasi K-NN, NB dan DT pada APK Android,” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 1, pp. 486–503, 2022, doi: 10.35957/jatisi.v9i1.1542.

[27] I. H. Sarker, M. H. Furhad, and R. Nowrozy, “AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions,” *SN Comput. Sci.*, vol. 2, no. 3, 2021, doi: 10.1007/s42979-021-00557-0.

[28] A. L. Samuel, “Some Studies in Machine Learning Using the Game of Checkers,” *IBM J. Res. Dev.*, vol. 3, no. 3, pp. 210–229, 1959, [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5392560

[29] S. Agarwal, *Data mining: Data mining concepts and techniques*. 2014. doi: 10.1109/ICMIRA.2013.45.

[30] F. E. Witten IH, *Data mining; Practical machine learning tools and techniques*. 2005.

[31] D. X. Dua S, *Data mining and machine learning in cybersecurity*. 2016. [Online]. Available: https://www.ptonline.com/articles/how-to-get-better-mfi-results

[32] U.-H. Tayyab, F. B. Khan, M. H. Durad, A. Khan, and Y. S. Lee, "A Survey of the Recent Trends in Deep Learning Based Malware Detection," *J. Cybersecurity Priv.*, vol. 2, no. 4, pp. 800–829, 2022, doi: 10.3390/jcp2040041.

[33] Y. Xin *et al.*, "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[34] I. H. Sarker, A. S. M. Kayes, and P. Watters, "Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage," *J. Big Data*, vol. 6, no. 1, 2019, doi: 10.1186/s40537-019-0219-y.

[35] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015, doi: 10.1038/nature14539.

[36] I. M. Coelho, V. N. Coelho, E. J. d. S. Luz, L. S. Ochi, F. G. Guimarães, and E. Rios, "A GPU deep learning metaheuristic based model for time series forecasting," *Appl. Energy*, vol. 201, pp. 412–418, 2017, doi: 10.1016/j.apenergy.2017.01.003.

[37] W. J. Deng, W. C. Chen, and W. Pei, "Back-propagation neural network based importance-performance analysis for determining critical service attributes," *Expert Syst. Appl.*, vol. 34, no. 2, pp. 1115–1125, 2008, doi: 10.1016/j.eswa.2006.12.016.

[38] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning Internal Representations by Error Propagation," *Readings Cogn. Sci. A Perspect. from Psychol. Artif. Intell.*, pp. 399–421, 2013, doi: 10.1016/B978-1-4832-1446-7.50035-2.

[39] N. M. Nawi, M. Z. Rehman, and A. Khan, "A New Bat Based Back-Propagation (BAT-BP) Algorithm," *Adv. Intell. Syst. Comput.*, vol. 240, pp. 395–404, 2014, doi: 10.1007/978-3-319-01857-7.

[40] D. Wu, Z. Yang, and L. Liang, “Using DEA-neural network approach to evaluate branch efficiency of a large Canadian bank,” *Expert Syst. Appl.*, vol. 31, no. 1, pp. 108–115, 2006, doi: 10.1016/j.eswa.2005.09.034.

[41] J. Li, J. Cheng, J. Shi, and F. Huang, “Brief Introduction of Back Propagation (BP) Neural Description of BP Algorithm in Mathematics,” *Adv. Comput. Sci. Inf. Eng.*, vol. 2, pp. 553–558, 2012.

[42] K. K. Al-jabery, T. Obafemi-Ajayi, G. R. Olbricht, and D. C. Wunsch II, “Selected approaches to supervised learning,” *Comput. Learn. Approaches to Data Anal. Biomed. Appl.*, pp. 101–123, 2020, doi: 10.1016/b978-0-12-814482-4.00004-8.

[43] M. Nielsen, *Neural Networks and Deep Learning*. Determination Press, 2015. doi: 10.1108/978-1-83909-694-520211010.

[44] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[45] C. Nwankpa, W. Ijomah, A. Gachagan, and S. Marshall, “Activation Functions: Comparison of trends in Practice and Research for Deep Learning,” pp. 1–20, 2018, [Online]. Available: http://arxiv.org/abs/1811.03378

[46] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, “Dropout: A simple way to prevent neural networks from overfitting,” *J. Mach. Learn. Res.*, vol. 15, no. 6, pp. 1929–1958, 2014, doi: 10.1016/0010-4361(73)90803-3.

[47] M. Liu, D. Yao, Z. Liu, J. Guo, and J. Chen, “An Improved Adam Optimization Algorithm Combining Adaptive Coefficients and Composite Gradients Based on Randomized Block Coordinate Descent,” *Comput. Intell. Neurosci.*, vol. 2023, pp. 1–14, 2023, doi: 10.1155/2023/4765891.

[48] S. Ruder, “An overview of gradient descent optimization algorithms,” pp. 1–14, 2016, [Online]. Available: http://arxiv.org/abs/1609.04747

[49] J. Duchi, E. Hazan, and Y. Singer, “Adaptive subgradient methods for online learning and stochastic optimization,” *Journa lof Mach. Learn. Res.*, vol. 12, pp. 2121–2159, 2011.

[50] A. A. Chowdhury, A. Das, K. K. S. Hoque, and D. Karmaker, “A Comparative Study of Hyperparameter Optimization Techniques for Deep Learning,” *Proc. Int. Jt. Conf. Adv. Comput. Intell.*, no. January, pp. 509–521, 2022, doi: https://doi.org/10.1007/978-981-19-0332-8_38.

[51] M. Feurer and F. Hutter, *Hyperparameter Optimization*. 2019. doi: 10.1007/978-3-030-05318-5_1.

[52] A. Palacios Cuesta, “Hyperparameter Optimization for Large-scale Machine Learning,” 2018. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-21533

[53] R. Bermúdez-chacón, G. H. Gonnet, and K. Smith, “Automatic model selection and hyperparameter optimization of Supervised Machine Learning algorithms,” 2015. [Online]. Available: https://doi.org/10.3929/ethz-a-010558061

[54] V. Kotu and B. Deshpande, “Predictive Analytics and Data Mining: Concepts and Practice with RapidMiner,” in *Predictive Analytics and Data Mining*, 2015, pp. 257–273. doi: 10.1016/b978-0-12-801460-8.00008-2.

[55] J. VanderPlas, *Python Data Science Handbook: Essential Tools for Working with Data*. 2016.

[56] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*, 2nd Editio. 2019.

[57] Python.org, “The Python Logo.” https://www.python.org/community/logos/ (accessed Feb. 02, 2023).

[58] “What is Flask Python - Python Tutorial.” https://pythonbasics.org/what-is-flask-python/ (accessed Feb. 02, 2023).

[59] A. Ronacher, “Logo of the Flask webframework.” https://id.wikipedia.org/wiki/Berkas:Flask_logo.svg (accessed Feb. 02, 2023).

[60] J. P. Mueller and L. Massaron, *Python for Data Science For Dummies*, 2nd Editio., no. 1. John Wiley & Sons, Inc., 2019.

[61] “Google Colab.” https://research.google.com/colaboratory/faq.html (accessed Jun. 01, 2023).

[62] Google.com, “Google Colaboratory.” https://colab.research.google.com/notebook (accessed Jun. 01, 2023).

[63] Michael Kennedy and M. Harrison, *Effective PyCharm: Learn the PyCharm IDE with a Hands-on Approach*. 2019.

[64] JetBrains, “PyCharm Logo.” https://intellij-support.jetbrains.com/hc/en-us/community/posts/5909943756818-PyCharm-Logo-Update (accessed Jun. 01, 2023).

[65] J. VanderPlas, *Python Data Science Handbook: Essential Tools for Working with Data*. 2017.

[66] “Anaconda.” https://www.anaconda.com/ (accessed Jun. 01, 2023).

[67] D. Jayanth, “Malware-Detection-in-PE-files-using-Machine-Learning,” 2021. https://github.com/DasariJayanth/Malware-Detection-in-PE-files-using-Machine-Learning/tree/master/PE_Header(exe%2C dll files)

[68] G. Ciaburro, V Kishore Ayyadevara, and A. Perrier, *Hands-On Machine Learning on Google Cloud Platform*, vol. 6, no. August. Packt Publishing Ltd, 2018.

[69] H. Hashemi, A. Azmoodeh, A. Hamzeh, and S. Hashemi, “Graph embedding as a new approach for unknown malware detection,” *J. Comput. Virol. Hacking Tech.*, vol. 13, no. 3, pp. 153–166, 2017, doi: 10.1007/s11416-016-0278-y.

[70] Microsoft Corporation, “Microsoft Portable Executable and Common Object File Format Specification,” 1999