

## DAFTAR PUSTAKA

- [1] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Computers and Security*, vol. 132. Elsevier Ltd, Sep. 01, 2023, Art. no. 103387. doi: 10.1016/j.cose.2023.103387.
- [2] Z. Wang, X. Ren, S. Li, B. Wang, J. Zhang, and T. Yang, "A Malicious URL Detection Model Based on Convolutional Neural Network," *Security and Communication Networks*, vol. 2021, 2021, Art. no. 5518528. doi: 10.1155/2021/5518528.
- [3] H. Ghalechyan, E. Israyelyan, A. Arakelyan, G. Hovhannisyan, and A. Davtyan, "Phishing URL detection with neural networks: an empirical study," *Scientific Reports*, vol. 14, no. 1, pp. 1–12, Dec. 2024, doi: 10.1038/s41598-024-74725-6.
- [4] S. U. Amin, "Phishing—A Cyber Fraud: The Types, Implications and Governance," *International Journal of Educational Reform*, vol. 33, no. 1, pp. 101–121, 2024, doi: 10.1177/10567879221082966.
- [5] A. A. Albishri and M. M. Dessouky, "A Comparative Analysis of Machine Learning Techniques for URL Phishing Detection," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18495–18501, 2024, doi: 10.48084/etasr.8920
- [6] F. Türk and M. Kılıçaslan, "Malicious URL detection with advanced machine learning and optimization-supported deep learning models," *Applied Sciences*, vol. 15, no. 18, Art. no. 10090, 2025, doi: 10.3390/app151810090.
- [7] P. S. Prasad, A. Kalamkar, M. Nagpure, N. Vaidya, P. Mohadikar, and B. Tembhurne, "Phishing URL Detection Using XGBoost and Custom Feature Engineering," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 13, no. V, pp. 675–686, May 2025, doi: 10.22214/ijraset.2025.70277.
- [8] K. S. Jishnu and B. Arthi, "Real-time phishing URL detection framework using knowledge distilled ELECTRA," *Automatika*, vol. 65, no. 4, pp. 1621–1639, 2024, doi: 10.1080/00051144.2024.2415797.
- [9] O. A. Akanbi, I. S. Amiri, and E. Fazeldehkordi, *Cyber security: A Machine-Learning Approach to Phishing Detection and Defense*, Rockland, MA, USA: Syngress, 2014.
- [10] Lukito and W. B. T. Handaya, "Deteksi Website Phishing Menggunakan Teknik Machine Learning," *Jurnal Informatika Atma Jogja*, vol. 6, no. 1, pp. 69–80, May 2025, doi: 10.24002/jiaj.v6i1.11538.
- [11] R. G. Guntara, "Aplikasi Deteksi Phishing Berbasis Android Menggunakan Metode Pengembangan Perangkat Lunak DSRM," *Jurnal Minfo Polgan*, vol. 12, no. 1, pp. 303–310, Mar. 2023, doi: 10.33395/jmp.v12i1.12379.

- [12] I. Mishchenko, "Phishing detection in Android applications using pretrained models and interface analysis," *Universum: Technical Sciences*, vol. 134, no. 5, pp. 15-19, May 2025. doi: 10.32743/UniTech.2025.134.5.20033.
- [13] M. A. Nielsen, *Neural Networks and Deep Learning*, San Francisco, CA, USA: Determination Press, 2015.
- [14] W. S. K. Ajjam and A. A. Ibrahim, "Enhanced Phishing URL Identification through Recurrent Neural Networks: A Comparative Study of LSTM and BiLSTM," *Journal of Queen College of Science and Mathematics*, vol. 17, no. 3, pp. 86–101, 2025, doi: 10.29304/jqcs.2025.17.32380.
- [15] O. Theobald, *Machine Learning for Absolute Beginners: A Plain English Introduction*, Tokyo, Japan: Independently Published, 2018.
- [16] M. Krichen and A. Mihoub, "Long Short-Term Memory Networks: A Comprehensive Survey," *AI*, vol. 6, p. 215, Sep. 2025, doi: 10.3390/ai6090215.
- [17] B. Tuychiyev, "LSTM Models: A Complete Guide to Long Short-Term Memory Networks," *DataCamp*, 2026. [Online]. Available: <https://www.datacamp.com/tutorial/lstm-models>. Accessed: Apr. 25, 2026.
- [18] S. Hartshorn, *Machine Learning with Random Forests and Decision Trees: A Visual Guide for Beginners*, Kindle ed. Seattle, WA, USA: Amazon Digital Services LLC, 2016.
- [19] R. Fauzan, A. V. Vitianingsih, D. Cahyono, A. L. Maukar, and Y. A. B. Suprio, "Penerapan Algoritma Klasifikasi pada Machine Learning untuk Deteksi Phishing," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 2, pp. 531–540, Mar. 2025, doi: 10.57152/malcom.v5i2.1968.
- [20] S. Sruthi, "Random Forest Algorithm in Machine Learning," *Analytics Vidhya*, 2025. [Online]. Available: <https://www.analyticsvidhya.com/blog/2021/06/understanding-random-forest/>. Accessed: Apr. 28, 2026.
- [21] Y. Perdana, "Comparative Analysis of Random Forest and XGBoost for Detecting Phishing Websites: A Machine Learning Approach," *Jurnal Kridatama Sains dan Teknologi*, vol. 7, no. 2, pp. 906–921, Dec. 2025, doi: 10.53863/kst.v7i02.1933.
- [22] J. Brownlee, *XGBoost with Python: Gradient Boosted Trees with XGBoost and scikit-learn*, Kindle ed. Melbourne, Australia: Machine Learning Mastery, 2016.
- [23] A. R. Kamila, F. Adikara, S. Sutrisno, and C. Herdian, "Analisa Pengaruh Penambahan Fitur dengan Perbandingan Algoritma berbasis Bagging dan Boosting pada Deteksi Phishing Link," *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, vol. 10, no. 3, pp. 460–467, Dec. 2024, doi: 10.26418/jp.v10i3.83366.

- [24] GeeksforGeeks, “XGBoost,” 2026. [Online]. Available: <https://www.geeksforgeeks.org/machine-learning/xgboost/>. Accessed: Apr. 28, 2026.
- [25] Elsevier, “Mendeley Data for journals,” Elsevier, [Online]. Available: <https://www.elsevier.com/researcher/author/tools-and-resources/research-data/mendeley-data-for-journals#0--about-mendeley-data>. Accessed: Apr. 30, 2026.
- [26] Microsoft, “Visual Studio Code: Get Started Overview,” 2026. [Online]. Available: <https://code.visualstudio.com/docs/getstarted/overview>. Accessed: Jun. 18, 2026.
- [27] JetBrains, “Kotlin for Android,” 2025. [Online]. Available: <https://kotlinlang.org/docs/android-overview.html>. Accessed: Apr. 30, 2026.
- [28] PcHardwarePro, “What is Android Studio: A Complete Guide to the Official IDE,” 2025. [Online]. Available: <https://www.pchardwarepro.com/en/What-is-Android-Studio-Complete-guide-to-the-official-IDE/>. Accessed: Apr. 30, 2026.
- [29] Railway, “Platform Overview,” 2026. [Online]. Available: <https://docs.railway.com/platform>. Accessed: Jun. 18, 2026.
- [30] PostgreSQL Global Development Group, “About PostgreSQL,” 2026. [Online]. Available: <https://www.postgresql.org/about/>. Accessed: Jun. 17, 2026.
- [31] V. Tiwari, S. Upadhyay, J. K. Goswami, and S. Agrawal, “Analytical Evaluation of Web Performance Testing Tools: Apache JMeter and SoapUI,” 12th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Jun. 2023, pp. 519–523, doi: 10.1109/CSNT57126.2023.10134699.
- [32] Apache Software Foundation, Apache JMeter, Wilmington, DE, USA: Apache Software Foundation. [Online]. Available: <https://jmeter.apache.org/index.html>. Accessed: Jun. 13, 2026.
- [33] CloudFactory, “Dataset Split in Machine Learning,” 2026. [Online]. Available: <https://wiki.cloudfactory.com/docs/mp-wiki/splits/data-splitting-in-machine-learning>. Accessed: Jun. 21, 2026.