DAFTAR PUSTAKA

[1] M. Khairi, B. Rianto, Chrismondari, Yolnasdi, M. Jalil, H. Juita, and E. Sudeska, "Pengaruh Teknologi Dalam Transformasi Ekonomi Dan Bisnis Di Era Digital," *Jurnal Perangkat Lunak*, vol. 7, no. 1, pp. 71–78, Feb. 2025, doi: 10.32520/jupel.v7i1.3947.

[2] L. A. Febrika Ardy, I. Istiqomah, A. E. Ezer, and S. N. Neyman, "*Phishing* di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 11, Jun. 2024, doi: 10.47134/pjise.v1i4.2753.

[3] D. Z. Oktavia, D. A. Hidayat, D. Natalia, S. K. Prabantara, and A. Arfriandi, "Perbandingan Performa Pembelajaran Mesin untuk Deteksi Ancaman Keamanan Aplikasi Web: Tinjauan Sistematis," *Jurnal Ilmiah Sistem Informasi*, vol. 5, no. 1, pp. 326–339, Jan. 2026, doi: 10.51903/dhayjg79.

[4] M. A. Pandu W, R. E. Saputro, P. Purwadi, and U. A. Rohmah, "Analisis Tingkat Akurasi Metode Naive Bayes dan *Random Forest* dalam Prediksi Penjualan Emas," *Jurnal Pendidikan dan Teknologi Indonesia*, vol. 5, no. 7, pp. 1809–1821, Jul. 2025, doi: 10.52436/1.jpti.732.

[5] S. Utomo, S. Sigit, N. Sulistyowati, D. A. Prasetya, and T. M. Fahrudin, "Perbandingan Kinerja Algoritma *XGBoost* dan CatBoost dalam Klasifikasi Risiko Penyakit Diabetes," *ALINIER: Journal of Artificial Intelligence & Applications*, vol. 6, no. 2, pp. 83–96, Nov. 2025, doi: 10.36040/alinier.v6i2.14772.

[6] A. Almomani, "*Phishing* Website Detection With Semantic Features Based on *Machine Learning* Classifiers," *Int. J. Semant. Web Inf. Syst.*, vol. 18, no. 1, pp. 1–24, Feb. 2022, doi: 10.4018/IJSWIS.297032.

[7] Q. E. ul Haq, M. H. Faheem, and I. Ahmad, "Detecting *Phishing* URLs Based on a Deep Learning Approach to Prevent Cyber-Attacks," *Applied Sciences*, vol. 14, no. 22, p. 10086, Nov. 2024, doi: 10.3390/app142210086.

[8] F. H. C. Adikara, "Pengaruh Penambahan Fitur dengan Perbandingan Algoritma berbasis Bagging dan Boosting pada Deteksi *Phishing* Link Ahya Radiatul Kamila, Analisa," *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, 2024.

[9] 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. 02, pp. 906–921, Dec. 2025, doi: 10.53863/kst.v7i02.1933.

[10] H. Ghalechyan, E. Israyelyan, A. Arakelyan, G. Hovhannisyan, and A. Davtyan, "*Phishing* URL detection with neural networks: an empirical study," *Sci. Rep.*, 2024, doi: 10.1038/s41598-024-74725-6.

[11] S. Sankaranarayanan, A. T. Sivachandran, A. S. Mohd Khairuddin, K. Hasikin, and A. R. Wahab Sait, "An ensemble classification method based on *Machine Learning* models for malicious Uniform Resource Locators (URL)," *PLoS One*, 2024, doi: 10.1371/journal.pone.0302196.

[12] M. Naseer, F. Ullah, S. Saeed, F. Algarni, and Y. Zhao, "Explainable TabNet ensemble model for identification of obfuscated URLs with features selection to ensure secure web browsing," *Sci. Rep.*, 2025, doi: 10.1038/s41598-025-93286-w.

[13] R. Gobinath and S. Manikandan, "Deep learning-based *Phishing* classification framework for accurate detection using optimized URL intelligence," *Sci. Rep.*, 2026, doi: 10.1038/s41598-026-46481-2.

[14] V. Ravula and M. Ramaiah, "Enhancing *Phishing* detection with dynamic optimization and character-level deep learning in cloud environments," *PeerJ Comput. Sci.*, 2025, doi: 10.7717/peerj-cs.2640.

[15] Z. Nurlan, D. Gabdullayev, B. Mukhametzhanova, N. Zhakiyev, I. Sonny, M. A. Ala'anzy, Z. Ahmad, and B. Amirgaliyev, "Incident-aware smart prioritization framework for penetration testing and prevention of URL-based cybersecurity attacks in industry 4.0 IoT networks," *Sci. Rep.*, 2025, doi: 10.1038/s41598-025-21409-4.

[16] A. Jain, S. Khan, K. Koli, H. Taneja, A. Panwar, T. Alshammari, E. M. Obaid, and S. M. Abdu, "PhishNet 1.0: optuna-optimized stacking ensemble with Boruta-based feature selection for *Phishing* URL detection," *Sci. Rep.*, 2025, doi: 10.1038/s41598-025-31447-7.

[17] M. Nauman, H. M. Usman Akhtar, H. Gorbani, M. Hadi Ul Hassan, and M. A. B. Fayyaz, "Transparent and trustworthy CyberSecurity: an XAI-integrated big data framework for *Phishing* attack detection," *Front. Big Data*, vol. 8, 2025, doi: 10.3389/fdata.2025.1688091.

[18] D. M. Linh and T. C. Hung, “A feature-engineered dataset of benign and *Phishing* URLs for *Machine Learning* and large language models evaluation,” *Data Brief*, vol. 59, 2025, doi: 10.1016/j.dib.2025.112162.

[19] H. P. Fitrian, W. Waryani, and N. R. Kirana, “Analisis Keamanan Jaringan Komputer Terhadap Ancaman Phising pada Pengguna E-Commerce,” *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 7, no. 6, Dec. 2024, doi: 10.32672/jnkti.v7i6.8388.

[20] G. A. Wiranata, Y. Ucuk, Subekti, and D. D. Sidarta, “Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana *Phishing*,” *Court Review: Jurnal Penelitian Hukum (e-ISSN: 2776-1916)*, vol. 4, no. 02, pp. 13–25, Mar. 2024, doi: 10.69957/cr.v4i02.1503.

[21] P. Sari and T. Sutabri, “Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari,” *Jurnal Digital Teknologi Informasi*, vol. 6, no. 1, p. 29, Mar. 2023, doi: 10.32502/digital.v6i1.5620.

[22] D. B. Suwarno and M. Hardjianto, “Deteksi Website *Phishing* Dari Analisis Url Menggunakan Algoritma *Random Forest*,” *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, vol. 21, no. 2, pp. 145–152, Sep. 2024, doi: 10.36080/bit.v21i2.3603.

[23] A. Saleem Raja, S. Peerbashab, Y. Mohammed Iqbal, B. Sundarvadivazhagan, and M. Mohamed Surputheen, “Structural Analysis of URL For Malicious URL Detection Using *Machine Learning*,” *JOURNAL OF ADVANCED APPLIED SCIENTIFIC RESEARCH*, vol. 5, no. 4, pp. 28–41, Jul. 2023, doi: 10.46947/joaasr542023679.

[24] Y. S. M. Gurning, D. Kiswanto, L. K. Daulay, and A. K. Nasution, “Sistem Klasifikasi Url Untuk Deteksi Situs Berbahaya Berbasis Analisis Fitur Jaringan,” *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 14, no. 1, Jan. 2026, doi: 10.23960/jitet.v14i1.8186.

[25] P. A. Firnanda, L. Shofwatillah, F. Rahma, and F. Fauzi, “Analisis Perbandingan Decision Tree dan *Random Forest* dalam Klasifikasi Penjualan Produk pada Supermarket,” *Emerging Statistics and Data Science Journal*, vol. 3, no. 1, pp. 445–461, Jan. 2025, doi: 10.20885/esds.vol3.iss.1.art2.

[26] S. Amaliah, M. Nusrang, and A. Aswi, “Penerapan Metode *Random Forest* Untuk Klasifikasi Varian Minuman Kopi di Kedai Kopi Konijiwa Bantaeng,” *VARIANSI: Journal of Statistics and Its application on Teaching and Research*, vol. 4, no. 3, pp. 121–127, Dec. 2022, doi: 10.35580/variansiunm31.

[27] F. A. K. Hidayat, N. Sulistianingsih, and R. Hammad, “Perbandingan Algoritma *XGBoost* dan *Random Forest* dalam Klasifikasi Surat Masuk Pemerintahan,” *RIGGS: Journal of Artificial Intelligence and Digital Business*, vol. 4, no. 4, pp. 10390–10397, Jan. 2026, doi: 10.31004/riggs.v4i4.5044.

[28] A. Pradana and S. Susanto, “Implementasi Model <i>Machine Learning</i> untuk Deteksi <i>Phishing</i> dengan Pendekatan Ekstraksi Fitur yang Dioptimalkan,” *Jurnal Teknologi Informasi dan Multimedia*, vol. 8, no. 1, pp. 27–40, Jan. 2026, doi: 10.35746/jtim.v8i1.881.

[29] E. R. Susanto, M. R. Inzaghi, A. Amarudin, and N. Neneng, “Evaluasi Kinerja Model *Random Forest* Dalam Memprediksi Diabetes Berdasarkan Dataset Kesehatan di Indonesia,” *Jurnal Pendidikan dan Teknologi Indonesia*, vol. 5, no. 7, pp. 1857–1866, Jul. 2025, doi: 10.52436/1.jpti.871.

[30] H. Kibriya, R. Amin, S. S. Alshamrani, S. Rehman, M. Hassan, and F. S. Alsubaei, “Lightweight malicious URL detection using deep learning and large language models,” *Sci. Rep.*, vol. 15, no. 1, p. 43044, Dec. 2025, doi: 10.1038/s41598-025-26653-2.

[31] B. Liu, J. Wu, H. Peng, A. Zhou, J. Wang, Q. Chen, and G. Tsoumakas, “Addressing Imbalance in Multi-Label Data via Label-Specific Distance-based Oversampling,” Jun. 2026, [Online]. Available: http://arxiv.org/abs/2606.05927

[32] U. Uche Emmanuel and F. Gideon Oghie, “A Lightweight Hybrid MLP-Based Framework for Real-Time *Phishing* URL Detection Using Structural URL Features.”

[33] G. Song, K. N. Khanghah, A. Patel, R. Malhotra, and H. Xu, “Physics-Distilled Neural Network enabled by Large Language Models for Manufacturing Process-Property Predictive Modeling.”

[34] P. C. . Bruce, Andrew. Bruce, and Peter. Gedeck, *Practical statistics for data scientists : 50+ essential concepts using R and Python* . O’Reilly Media, Inc., 2020.

[35] C. Bentéjac, A. Csörgő, and G. Martínez-Muñoz, "A comparative analysis of gradient boosting algorithms," *Artif. Intell. Rev.*, vol. 54, no. 3, pp. 1937–1967, Mar. 2021, doi: 10.1007/s10462-020-09896-5.

[36] J. Liu, J. Bu, X. Han, Z. Wang, D. Dong, M. Wei, and Q. Wu., "Development of *Machine Learning*-based predictive models for fertility intentions in patients with Crohn's disease," *Frontiers in Reproductive Health*, vol. 8, May 2026, doi: 10.3389/frph.2026.1836350.