

DAFTAR PUSTAKA

- [1] Kelas 4A4 and O. Iskandar, "ANALISIS KEJAHATAN ONLINE PHISHING PADA MASYARAKAT," *Leuser: Jurnal Hukum Nusantara*, vol. 1, no. 2, pp. 32–36, May 2024.
- [2] P. J. Uppalapati, B. K. Gontla, P. Gundu, S. M. Hussain, and K. Narasimharo, "A Machine Learning Approach to Identifying Phishing Websites: A Comparative Study of Classification Models and Ensemble Learning Techniques," *EAI Endorsed Scal Inf Syst*, Jun. 2023, doi: 10.4108/eetsis.vi.3300.
- [3] M. W. Shaukat, R. Amin, M. M. A. Muslam, A. H. Alshehri, and J. Xie, "A Hybrid Approach for Alluring Ads Phishing Attack Detection Using Machine Learning," *Sensors (Basel)*, vol. 23, no. 19, p. 8070, Sep. 2023, doi: 10.3390/s23198070.
- [4] S. K. Ahmad, B. A. Dapshima, and Y. C. Essa, "Detection of Phishing Attacks Using Machine Learning Techniques," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 06, no. 07, pp. 1166–1176, Jul. 2024, doi: 10.56726/IRJMETS60054.
- [5] D. B. Suwarno and M. Hardjianto, "DETEKSI WEBSITE PHISHING DARI ANALISIS URL MENGGUNAKAN ALGORITMA RANDOM FOREST," 2024.
- [6] M. Sholeh, U. Lestari, and D. Andayati, "Comparison of Feature Selection with Information Gain Method in Decision Tree, Regression Logistic and Random Forest Algorithms," *JABT*, vol. 5, no. 3, pp. 146–153, Sep. 2024, doi: 10.35145/jabt.v5i3.155.
- [7] T. A. Y. Siswa and W. J. Pranoto, "Implementasi Seleksi Fitur Information Gain Ratio pada Algoritma Random Forest untuk Model Data Klasifikasi Pembayaran Kuliah," *Dinamika Informatika*, vol. 15, no. 1, pp. 41–49, Mar. 2023.
- [8] M. D. Aprima, E. Budianita, F. Syafria, and I. Afrianty, "PENERAPAN METODE INFORMATION GAIN DAN LEARNING VECTOR QUANTIZATION 3 PADA KLASIFIKASI PENYAKIT GINJAL," *INFOS Journal*, vol. 8, no. 01, pp. 29–39, Jun. 2025, doi: 10.24076/infosjournal.2025v8i01.2117.

- [9] M. Hasibuan, R. Abdillah, S. Agustian, and R. M. Candra, "Classification of Phishing URL Attacks Using Random Forest Algorithm Based on Feature Importance," *bit-Tech (Binary Digital - Technology)*, vol. 8, no. 2, pp. 2984–2993, Dec. 2025, doi: 10.32877/bt.v8i2.3511.
- [10] B. B. Gupta *et al.*, "A Hybrid CNN-Brown-Bear Optimization Framework for Enhanced Detection of URL Phishing Attacks," *CMC*, vol. 81, no. 3, pp. 4853–4874, 2024, doi: 10.32604/cmc.2024.057138.
- [11] A. Safi and S. Singh, "A systematic literature review on phishing website detection techniques," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 2, pp. 590–611, Feb. 2023, doi: 10.1016/j.jksuci.2023.01.004.
- [12] A. D. Sulisty, B. D. Wicaksono, R. N. Saputra, and R. Ramadhani, "Strategi Penanggulangan Serangan Phishing di Media Sosial," 2024.
- [13] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, p. 563060, Mar. 2021, doi: 10.3389/fcomp.2021.563060.
- [14] H. Ghalechyan, E. Israyelyan, A. Arakelyan, G. Hovhannisyan, and A. Davtyan, "Phishing URL detection with neural networks: an empirical study," *Sci Rep*, vol. 14, no. 1, p. 25134, Oct. 2024, doi: 10.1038/s41598-024-74725-6.
- [15] A. Butnaru, A. Mylonas, and N. Pitropakis, "Towards Lightweight URL-Based Phishing Detection," *Future Internet*, vol. 13, no. 6, p. 154, Jun. 2021, doi: 10.3390/fi13060154.
- [16] J. S. Lee and Y. G. P. David, "TypoSwype: An Imaging Approach to Detect Typo-Squatting," in *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Apr. 2021, pp. 1–5. doi: 10.1109/NTMS49979.2021.9432673.
- [17] A. Kulkarni, V. Balachandran, and T. Das, "Phishing Webpage Detection: Unveiling the Threat Landscape and Investigating Detection Techniques," Sep. 10, 2025, *arXiv*: arXiv:2509.08424. doi: 10.48550/arXiv.2509.08424.
- [18] D. Li, Q. Chen, and L. Wang, "Phishing Attacks: Detection and Prevention Techniques," Aug. 2024, doi: 10.5281/ZENODO.12789572.

- [19] D. Kalla, "Phishing Detection Implementation using Databricks and Artificial Intelligence," *International Journal of Computer Applications*, vol. 185, no. 11, pp. 1–11, May 2023, doi: 10.5120/ijca2023922764.
- [20] R. Fauzan, A. V. Vitianingsih, D. Cahyono, A. L. Maukar, and Y. A. B. Suprio, "Penerapan Algoritma Klasifikasi pada Machine Learning untuk Deteksi Phishing: Application of Classification Algorithms in Machine Learning for Phishing Detection," *MALCOM*, vol. 5, no. 2, pp. 531–540, Mar. 2025, doi: 10.57152/malcom.v5i2.1968.
- [21] M. A. Ismail, H. H. Nuha, and S. M. Yasin, "Phishing Detection Using Machine Learning: Performance Evaluation of Classification Algorithms", *International Journal on Advanced Science, Engineering and Information Technology*, vol. 15, no. 5, pp. 1616–1622, 2025.
- [22] S. H. Rukiman and A. Rahmatulloh, "Evaluasi Efektivitas Penggunaan FastText Embedding dan LSTM Networks dalam Deteksi Phishing Email," *FaktorExacta*, vol. 18, no. 2, p. 194, Oct. 2025, doi: 10.30998/faktorexacta.v18i2.26769.
- [23] A. Pradana and S. Susanto, "Implementasi Model *Machine Learning* untuk Deteksi *Phishing* dengan Pendekatan Ekstraksi Fitur yang Dioptimalkan," *jtim*, vol. 8, no. 1, pp. 27–40, Jan. 2026, doi: 10.35746/jtim.v8i1.881.
- [24] M. Masanga, M. Lamine, and M. Ahmad, "ENHANCED PHISHING DETECTION USING MACHINE LEARNING AND URL ANALYSIS," 2026.
- [25] Q. E. U. 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.
- [26] D. Rathee and S. Mann, "Detection of E-Mail Phishing Attacks – using Machine Learning and Deep Learning," *IJCA*, vol. 183, no. 47, pp. 1–7, Jan. 2022, doi: 10.5120/ijca2022921868.
- [27] K. Omari, C. Taoussi, and A. Oukhatar, "Comparative Analysis of Undersampling, Oversampling, and SMOTE Techniques for Addressing Class Imbalance in Phishing Website Detection," *ijacsa*, vol. 16, no. 2, 2025, doi: 10.14569/IJACSA.2025.0160276.

- [28] Sohaib Latif and Saher Pervaiz, “DETECTING PHISHING ATTACKS IN CYBERSECURITY USING MACHINE LEARNING WITH DATA PREPROCESSING AND FEATURE ENGINEERING,” *Kashf J. Multidiscip. Res.*, vol. 2, no. 03, pp. 89–99, Mar. 2025, doi: 10.71146/kjmr335.
- [29] M. A. Daniel, S.-C. Chong, L.-Y. Chong, and K.-K. Wee, “Optimising Phishing Detection: A Comparative Analysis of Machine Learning Methods with Feature Selection,” *JIWE*, vol. 4, no. 1, pp. 200–212, Feb. 2025, doi: 10.33093/jiwe.2025.4.1.15.
- [30] I. Arifin and Chairani, “Phishing Website Detection Using a Machine Learning Classification Approach,” *Jurnal Inovtek Polbeng - Seri Informatika*, vol. 10, no. 3, pp. 1498–1508, Nov. 2025.
- [31] A. Almomani *et al.*, “Phishing Website Detection With Semantic Features Based on Machine Learning Classifiers: A Comparative Study,” *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1–24, Feb. 2022, doi: 10.4018/IJSWIS.297032.
- [32] A. Awasthi and N. Goel, “Efficient And Accurate Technique For Improving ML Classifier Performance Using Feature Selection In Phishing Website Prediction,” *Kuey*, 2023, doi: 10.53555/kuey.v29i4.4369.
- [33] F. Yang, Z. Xu, H. Wang, L. Sun, M. Zhai, and J. Zhang, “A hybrid feature selection algorithm combining information gain and grouping particle swarm optimization for cancer diagnosis,” *PLoS ONE*, vol. 19, no. 3, p. e0290332, Mar. 2024, doi: 10.1371/journal.pone.0290332.
- [34] M. I. Prasetyowati, N. U. Maulidevi, and K. Surendro, “The accuracy of Random Forest performance can be improved by conducting a feature selection with a balancing strategy,” *PeerJ Computer Science*, vol. 8, p. e1041, Jul. 2022, doi: 10.7717/peerj-cs.1041.
- [35] S. F. Ahmed *et al.*, “Deep learning modelling techniques: current progress, applications, advantages, and challenges,” *Artif Intell Rev*, vol. 56, no. 11, pp. 13521–13617, Nov. 2023, doi: 10.1007/s10462-023-10466-8.

- [36] M. I. Kamalamma, M. L. Devi, A. Reshmitha, K. L. Devi, and V. Sobha, "Phishing Detection System through Hybrid Machine Learning Based On URL," *International Journal of All Research Education and Scientific Methods (IJARESM)*, vol. 13, no. 4, pp. 153–163, Apr. 2025.
- [37] M. V. Vineeth and G. V. Ramana, "Detection of Phishing Websites Using Machine Learning", *Metallurgical and Materials Engineering*, vol. 31, no. 4, pp. 762–768, Apr. 2025, doi: 10.63278/1511.
- [38] P. J. Uppalapati, B. K. Gontla, P. Gundu, S. M. Hussain, and K. Narasimharo, "A Machine Learning Approach to Identifying Phishing Websites: A Comparative Study of Classification Models and Ensemble Learning Techniques," *EAI Endorsed Scal Inf Syst*, Jun. 2023, doi: 10.4108/eetsis.vi.3300.
- [39] P. Gayatri, A. Vaishnavi, G. Sahruthi, P. Varshini, and A. Nikshitha, "DETECTION OF FRAUDULENT WEBSITES USING MACHINE LEARNING," *JNAO*, vol. 14, no. 02, pp. 161–170, 2023, doi: 10.36893/JNAO.2023.V14I2.0161-0170.
- [40] P. Desai and M. Shah, "Phishing Website Detection Using Machine Learning: A Comprehensive Study", *International Journal For Multidisciplinary Research (IJFMR)*, vol. 5, no. 6, Nov.–Dec. 2023, doi: 10.36948/ijfmr.2023.v05i06.9711.
- [41] A. A. Albishri and M. M. Dessouky, "A Comparative Analysis of Machine Learning Techniques for URL Phishing Detection," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 6, pp. 18495–18501, Dec. 2024, doi: 10.48084/etasr.8920.
- [42] N. F. Almujaheed, M. A. Haq, and M. Alshehri, "Comparative evaluation of machine learning algorithms for phishing site detection," *PeerJ Computer Science*, vol. 10, p. e2131, Jun. 2024, doi: 10.7717/peerj-cs.2131.
- [43] A. Brissett and J. Wall, "Machine Learning and Watermarking for Accurate Detection of AI-Generated Phishing Emails," *Electronics*, vol. 14, no. 13, p. 2611, Jun. 2025, doi: 10.3390/electronics14132611.
- [44] N. Innab *et al.*, "Phishing Attacks Detection Using Ensemble Machine Learning Algorithms," *CMC*, vol. 80, no. 1, pp. 1325–1345, 2024, doi: 10.32604/cmc.2024.051778.

- [45] O. Faruq, F. Ahammed, A. S. Mily, and 4Ashraful Islam, “Machine Learning for Enhanced Churn Prediction in Banking: Leveraging Oversampling and Stacking Techniques,” *int.jour.sci.res.mana*, vol. 12, no. 09, pp. 1434–1446, Sep. 2024, doi: 10.18535/ijssrm/v12i09.ec03.
- [46] P. Sumanth, A. Vijay, D. N. Aravindh, and D. G. R. Nesakumari, “EARLY DIAGNOSIS AND PREDICTION OF FETAL ABNORMALITIES USING MACHINE LEARNING,” vol. 8, no. 5, 2023.
- [47] G. Airlangga, “Evaluating the Effectiveness of Machine Learning Models for Cyberattack Detection: A Study on Model Generalization and Dataset Imbalance,” *josh*, vol. 6, no. 1, pp. 619–628, Oct. 2024, doi: 10.47065/josh.v6i1.6089.
- [48] K. Anantha Lakshmi, S. Prashanth, and M. Narendra, “Machine Learning Model Selection for Banking & Insurance Applications Using Performance-Based Evaluation Metrics,” *IJSR*, pp. 1803–1807, Dec. 2025, doi: 10.21275/SR251222132524.
- [49] O. A. Montesinos López, A. Montesinos López, and J. Crossa, *Multivariate Statistical Machine Learning Methods for Genomic Prediction*. Cham: Springer International Publishing, 2022. doi: 10.1007/978-3-030-89010-0.
- [50] E. Halabaku and E. Bytyçi, “Overfitting in Machine Learning: A Comparative Analysis of Decision Trees and Random Forests,” *IASC*, vol. 39, no. 6, pp. 987–1006, 2024, doi: 10.32604/iasc.2024.059429.
- [51] Y. R. Rahmawan, H. Nurjaman, and F. F. Ramadhan, “High-Recall URL Phishing Detection via Multilayer Perceptron: Feature Selection, Learning Curves, and Confusion-Matrix Verification,” *BIMA*, vol. 1, no. 2, pp. 16–23, Jan. 2026, doi: 10.65780/bima.v1i2.9.
- [52] Department of Computer Science, Faculty of Natural and Applied Sciences Al-Hikmah University, Ilorin, Nigeria *et al.*, “Analysis of Single and Ensemble Machine Learning Classifiers for Phishing Attacks Detection,” *IJSECS*, vol. 7, no. 2, pp. 44–49, Aug. 2021, doi: 10.15282/ijsecs.7.2.2021.5.0088.
- [53] T. Choudhary, S. Mhapankar, R. Bhddha, A. Kharuk, and R. Patil, “Machine Learning Approach for Phishing Attack Detection,” *JAIT*, May 2023, doi: 10.37965/jait.2023.0197.

- [54] M. G. Awwad, M. M. Ashour, E. S. A. Marzouk, and E. Abdelhalim, “Anti-Phishing approach for IoT system in Fog networks based on machine learning algorithms,” *Mansoura Engineering Journal*, vol. 49, no. 3, Mar. 2024, doi: 10.58491/2735-4202.3196.

