# DAFTAR PUSTAKA


[1] Anti-*Phishing* Working Group (APWG), "*Phishing* Activity Trends Report Q4 2024," APWG, 2024. [Online].

[2] S. Hamadouche, O. Boudraa, and M. Gasmi, "Combining Lexical, Host, and Content-based Features for *Phishing Website*s Detection using *Machine learning* Models," Proceedings on Scalable Information Systems, vol. 11, no. 6, 2024.

[3] M. R. Islam, M. M. Islam, M. S. Afrin, A. Antara, N. Tabassum, and A. Amin, "PhishGuard: A Convolutional Neural Network-Based Model for Detecting *Phishing* URLs with Explainability Analysis," 2024.

[4] R. Wahyudi, "Hyperband-Optimized *LightGBM* and *Ensemble learning* for *Web Phishing* Detection with SHAP-Based Interpretability," Journal of Computer Science and Engineering (JCSE), vol. 6, no. 2, pp. 59–70, 2025.

[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.

[6] A. F. Mahmud and S. Wirawan, "Deteksi *Phishing Website* Menggunakan *Machine learning* Metode Klasifikasi," *Jurnal Sistemasi: Sistem Informasi*, vol. 13, no. 4, pp. 1156–1167, 2024.

[7] A. K. Kencana, F. D. Ananda, A. D. Hartanto, and Hartatik, "Implementasi Metode *Random Forest* Klasifikasi untuk *Phishing* Link Detection," *Intechno Journal: Information Technology Journal*, vol. 4, no. 2, pp. 69–74, 2022.

[8] S. Diantika, "Penerapan Teknik Random Oversampling untuk Mengatasi Imbalance Class dalam Klasifikasi *Website Phishing* Menggunakan Algoritma *LightGBM*," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 7, no. 1, pp. 19–25, 2023.

[9] L. I. Uzlah, R. A. Saputra, and Isnawaty, "Deteksi Serangan Siber Pada Jaringan Komputer Menggunakan Metode Random Forest," JATI (Jurnal Mahasiswa Teknik Informatika), vol. 8, no. 3, pp. 2787–2793, 2024.

[10] A. Kautsar, M. Aida, and A. Yulistia, "Applying Random Forest Algorithm for *Phishing* URL Identification," Journal of Computers and Digital Business, vol. 4, no. 3, 2025.

[11] V. V. K. Reddy, Y. N. Sai, T. Keerthi, and K. A. Reddy, "Detection of *Phishing Website* Using *Support Vector Machine* and *Light Gradient Boosting Machine learning Algorithms*," in *International Conference on Innovative Computing and Communication (ICICC 2023), Lecture Notes in Networks and Systems*, vol. 741, pp. 297–308, 2023

[12] R. Rumini, N. Norhikmah, A. Mustofa, and S. Pradana, "Perbandingan Pengujian Deteksi *Phishing* menggunakan Metode SVM dengan *Kernel* RBF dan Linear," *Jurnal Sistem Informasi*, vol. 12, no. 3, pp. 754–759, 2023.

[13] Fauzan, R., Vitianingsih, A. V., Cahyono, D., Maukar, A. L., & Suprio, Y. A. B., "Penerapan Algoritma Klasifikasi pada *Machine learning* untuk Deteksi *Phishing*," *Institut Riset dan Publikasi Indonesia*, vol. 5, no. 531-540, 2025.

[14] T. Bagies, "Classifying Software Security Requirements into Confidentiality, Integrity, and Availability Using Machine Learning Approaches," PeerJ Computer Science, vol. 10, e2554, 2024.

[15] T. Ahmad, Z. Tabrez, dan A. Warsi, "Regulatory Challenges of Cybersecurity and Privacy: A Threat to Digital Economy," *Proceedings of the International Conference on Law and Technology* (*ICLT 2025*), *Atlantis Press*, 2025.

[16] L. J. Adeyemo, I. O. David, dan T. Y. Olabulo, "Malware, Data Theft and Emotional Distress as Risk Factors of *Phishing* in Nigeria," *International Journal of Criminology* & *Justice* (*IJCJ*), vol. 1, no. 1, pp. 10-20, 2025.

[17] A. Aljofey, Q. Jiang, A. Rasool, H. Chen, W. Liu, Q. Qu, and Y. Wang, "An Effective Detection Approach for *Phishing* Websites Using URL and HTML Features," Scientific Reports, vol. 12, no. 1, Art. no. 8842, 2022.

[18] Alnemari and M. Alshammari, "Detecting *Phishing* Domains Using Machine Learning," Applied Sciences, vol. 13, no. 8, Art. no. 4649, 2023.

[19] A. K. Jain and B. B. Gupta, "A survey of *phishing* attack techniques, defence mechanisms and open research challenges," *Enterprise Information Systems*, vol. 16, no. 4, pp. 527–565, 2022.

[20] S. Kailas and R. Roopalakshmi, "'Think Before You Click'—Malicious *URL* Detection in Cybersecurity: A Systematic Review and Research Roadmap," IEEE Access, vol. 13, pp. 154305–154325, 2025, doi: 10.1109/ACCESS.2025.3601387.

[21] K. M. Sudar, M. Rohan, and K. Vignesh, “Detection of adversarial *phishing* attack using *machine learning* techniques,” Sādhanā, vol. 49, no. 232, 2024, doi: 10.1007/s12046-024-02582-0.

[22] J. Yu, A. V. Shvetsov, and S. H. Alsamhi, “Leveraging *machine learning* for cybersecurity resilience in industry 4.0: Challenges and future directions,” *IEEE Access*, vol. 12, pp. 159579–159596, 2024.

[23] M. Kayal, J. Patra, S. Kumar, J. Pati, L. K. Singh, and V. Sawan, “Enhancing Mental Health Treatment Prediction Using BXGBoost: A Hybrid *Machine learning* Approach,” *International Conference on Computing, Intelligence, and Application (CIACON)*, 2025.

[24] M. A. Ganaie, M. Hu, A. K. Malik, M. Tanveer, and P. N. Suganthan, "Ensemble deep learning: A review," *Engineering Applications of Artificial Intelligence*, vol. 115, p. 105151, 2022.

[25] R. A. Ahmed, W. El-Shafai, Z. A. Ahmed, and E. S. M. El-Rabaie, “High-*precision* crop recommendation system with stacking ensemble classifiers for optimizing agricultural productivity,” *Scientific Reports*, vol. 15, no. 43377, 2025.

[26] R. Reátegui, C. Tandazo-Malla, R. Suárez, and L. Ramírez-Cerna “Cardiovascular risk prediction via ensemble *machine learning* and oversampling methods,” *Scientific Reports*, vol. 15, no. 43576, 2025.

[27] A. Azibaev, “The Role of Gradient Boosting Machines in Modern Economic Analysis,” *Universum: Technical Sciences*, vol. 1, no. 130, 2025.

[28] I. A. Mahmoud, M. G. Abdullahi, and L. Garba, “Interpretable SHAP-Based Data-Driven Framework for Optimizing Treatment Performance Through Turbidity Dynamics Modelling,” *Techno-computing Journal*, vol. 1, no. 3, 2025.

[29] J. A. Ilemobayo, O. Durodola, O. Alade, O. J. Awotunde, A. T. Olanrewaju, O. Falana, A. Ogungbire, et al., “Hyperparameter Tuning in Machine Learning: A Comprehensive Review,” Journal of Engineering Research and Reports, vol. 26, no. 6, pp. 388–395, 2024.

[30] M. R. A. Yudianto, M. Zakariah, N. F. Rozam, D. F. Rahman, T. N. Sari, and Z. Mustofa, “Support Vector Machine Algorithm Optimization for Sentiment

Analysis using Bayesian Optimization," *Jurnal Teknik Informatika dan Sistem Informasi (JuTISI)*, vol. 11, no. 3, pp. 383–393, 2025.

[31] D. N. Sulistyowati, S. Hadianti, and N. A. Mayangky, "Comparison of Naive Bayes and Decision Tree Methods in Breast Cancer Classification," *MEDINFTech*, vol. 3, no. 4, pp. 143–148, 2025.

[32] O. Rainio, J. Teuho, and R. Klén, "Evaluation metrics and statistical tests for *machine learning*," Scientific Reports, vol. 14, no. 6086, 2024, doi: 10.1038/s41598-024-56706-x.

[33] K. Karoo, "The Indispensable Role of Python Programming in Modern Data Science," *International Journal of Computer Techniques*, vol. 12, no. 5, 2025.

[34] M. A. Mamun, M. A. Huraira, M. Begum, et al., "Research literacy and its predictors among university students and graduates identified by *machine learning* and spatial analysis," *Scientific Reports*, vol. 15, no. 35622, 2025.

[35] M. Aljabri, F. Alhaidari, R. M. A. Mohammad, S. Mirza, D. H. Alhamed, H. S. Altamimi, S. M. B. Chrouf, A. O. Alnajim, and S. A. Aldossary, "An assessment of lexical, network, and content-based features for detecting malicious *URL*s using *machine learning* and deep learning models," Computational Intelligence and Neuroscience, vol. 2022, Art. no. 3241216, pp. 1–14, 2022, doi: 10.1155/2022/3241216.

[36] M. Mia, D. Derakhshan, and M. M. A. Pritom, "Can Features for *Phishing URL* Detection Be Trusted Across Diverse Datasets? A Case Study with Explainable AI," *arXiv preprint*, 2024.

[37] I. Altan, A. Bachir, Y. Parbhulkar, A. M. Rizvi, and M. Farazi, "Dual-Path *Phishing* Detection: Integrating Transformer-Based NLP with Structural *URL* Analysis," *arXiv preprint*, 2025.

[38] R. A. Sodikin & R. Hikmawan, "Analysis of Gamification in Cybersecurity Education for Students: A Systematic Literature Review," *Jurnal Educative: Journal of Educational Studies*, vol. 8, no. 2, pp. 147-166, 2023.

[39] Y. A. A. S. Aldeen, F. K. Jabor, et al., "A Hybrid Heuristic AI Technique for Enhancing Intrusion Detection Systems in IoT Environments," *Journal of Intelligent Systems and Internet of Things*, vol. 14, no.1, pp. 1-15, 2025.

[40] TutorialsPoint, "*LightGBM* - Architecture," Tutorialspoint. [Online].