

DAFTAR PUSTAKA

- [1] B. Wibowo And T. Hidayat, “Strategi Efektif Dalam Meningkatkan Kesadaran Keamanan Siber Terhadap Ancaman Phishing Di Lingkungan Perusahaan Pt. Xyz,” *J. Pengabd. Masy. Sultan Indones.*, Vol. 2, No. 1, Pp. 1–9, 2024, Doi: 10.58291/Abdisultan.V2i1.294.
- [2] A. Al-Qasmi, A. Al-Anazi, L. Al-Shehri, S. A-Lshaman, And W. Al-Atawi, “Intelligent Systems And Applications In Engineering Machine Learning-Based Phishing Detection System,” Vol. 12, No. 4, Pp. 4367–4372, 2024.
- [3] A. Bezerra *Et Al.*, “A Case Study On Phishing Detection With A Machine Learning Net,” *Int. J. Data Sci. Anal.*, 2024, Doi: 10.1007/S41060-024-00579-W.
- [4] J. J. M. L. Piñeiro And L. R. Wong Portillo, “Web Architecture For Url-Based Phishing Detection Based On Random Forest, Classification Trees, And Support Vector Machine,” *Intel. Artif.*, Vol. 25, No. 69, Pp. 107–121, 2022, Doi: 10.4114/Intartif.Vol25iss69pp107-121.
- [5] A. K. Kencana, F. D. Ananda, A. D. Hartanto, And H. Hartatik, “Implementasi Metode Random Forest Klasifikasi Untuk Phishing Link Detection,” *Intechno J. (Information Technol. Journal)*, Vol. 4, No. 2, Pp. 55–59, 2022, Doi: 10.24076/Intechnojournal.2022v4i2.1562.
- [6] Sridevi Malipatil, A S Kruthik, Eldad Nischal, G S Vinay Kumar, And Ajay Kumar H A, “Detection Of Phishing Website Using Xg – Boost Algorithm,” *Int. J. Adv. Res. Sci. Commun. Technol.*, Pp. 437–440, 2024, Doi:

10.48175/Ijarsct-18165.

- [7] S. Anjum, T. Uma Devi, K. K. Namish, And B. Vasundhara Devi, “Phishing Website Detection Paradigm Using Xgboost,” *Int. Res. J. Eng. Technol.*, Vol. 9, No. 12, Pp. 1364–1367, 2022, [Online]. Available: [Www.Irjet.Net](http://www.Irjet.Net)
- [8] A. N. Rachmi, “Implementasi Metode Random Forest Dan Xgboost Pada Klasifikasi Customer Churn,” Pp. 1–101, 2020.
- [9] K. Pagadala, “Detecting Phishing Sites Without Visiting Them,” Pp. 1–15, 2022.
- [10] A. Khairunnisa, “Perbandingan Model Random Forest Dan Xgboost Untuk Prediksi Kejahatan Kesusilaan Di Provinsi Jawa Barat,” *Jiko (Jurnal Inform. Dan Komputer)*, Vol. 7, No. 2, P. 202, 2023, Doi: 10.26798/Jiko.V7i2.799.
- [11] F. D. U. Arif, *Perbandingan Kinerja Algoritma Random Forest, Xgboost Dan Lightgbm Dalam Klasifikasi Emosi Komentar Reddit*. 2023.
- [12] D. Phishing, A. R. Kamila, F. Adikara, And C. Herdian, “Analisa Pengaruh Penambahan Fitur Dengan Perbandingan Algoritma Berbasis Bagging Dan Boosting Pada Deteksi Phishing Link,” Vol. 10, No. 3, Pp. 460–467, 2024.
- [13] R. D. Hapsari And K. G. Pambayun, “Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis,” *J. Konstituen*, Vol. 5, No. 1, Pp. 1–17, 2023, Doi: 10.33701/Jk.V5i1.3208.
- [14] K. Barik, S. Misra, And R. Mohan, “Web-Based Phishing Url Detection Model Using Deep Learning Optimization Techniques,” *Int. J. Data Sci. Anal.*, No. C, 2025, Doi: 10.1007/S41060-025-00728-9.
- [15] V. A. Windarni, A. F. Nugraha, S. T. A. Ramadhani, D. A. Istiqomah, F. M.

- Puri, And A. Setiawan, "Deteksi Website Phishing Menggunakan Teknik Filter Pada Model Machine Learning," *Inf. Syst. J.*, Vol. 6, No. 01, Pp. 39–43, 2023, Doi: 10.24076/Infosjournal.2023v6i01.1268.
- [16] Irfan Fanasafa, "Anda, Waspada! Kehajatan Phising Mengintai," Kementrian Keuangan.
- [17] S. M. Wajid, T. Javed, And M. Mohd Su'ud, "Ensemble Learning-Powered Url Phishing Detection: A Performance Driven Approach," *J. Informatics Web Eng.*, Vol. 3, No. 2, Pp. 134–145, 2024, Doi: 10.33093/Jiwe.2024.3.2.10.
- [18] A. F. Mahmud And S. Wirawan, "Phishing Website Detection Using Machine Learning Classification Method," *Sistemasi*, Vol. 13, No. 4, P. 1368, 2024, Doi: 10.32520/Stmsi.V13i4.3456.
- [19] M. Adnan, "Penggunaan Machine Learning Dan Analisis Data Pada Lms/Alms," *Skripsi*, Pp. 7–51, 2021.
- [20] N. Sitohang, "Perbandingan Algoritma Random Forest, Naive Bayes, Dan Neural Network Dalam Klasifikasi Penyakit Jantung," *Penerapan Data Min. Untuk Peringatan Dini Banjir Menggunakan Metod. Klastering K-Means*, Vol. 2, No. 1, Pp. 16–20, 2023.
- [21] Asiva Noor Rachmayani, *Pengantar Machine Learning*. 2022.
- [22] Y. Jinana, Dan Kusnawi, And P. Informatika Universitas Amikom Yogyakarta Yogyakarta, "Klasifikasi Random Forest Terhadap Diagnosa Penyakit Kanker Payudara Berdasarkan Status Keganasan (Random Forest Classification Of Breast Cancer Disease Diagnosis Based On Malignancy

Status),” Pp. 129–134.

- [23] S. K. Birthriya, P. Ahlawat, And A. K. Jain, “Phishing Website Detection With Xgboost And Adaptive Hyperparameter Optimization Using The Bat Algorithm,” *Procedia Comput. Sci.*, Vol. 258, Pp. 1774–1782, 2025, Doi: 10.1016/J.Procs.2025.04.429.
- [24] I. G. Agus, K. Warmayana, And Y. Yamashita, “Predicting Cyber Attack Types Using Xgboost: A Data Mining Approach To Enhance Legal Frameworks For Cybersecurity,” Vol. 1, No. 2, Pp. 147–160, 2025, Doi: 10.63913/Jcl.V1i2.8.
- [25] V. Yolanda And E. Setiawan, “Klasifikasi Air Layak Konsumsi Berdasarkan Ph, Kekeruhan, Dan Konsentrasi Zat Terlarut Berbasis Arduino Menggunakan Random Forest,” *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, Vol. 1, No. 1, P. 3, 2017.
- [26] S. J. Sari, D. Syauqy, And W. Kurniawan, “Klasifikasi Kelayakan Konsumsi Air Kelapa Berdasarkan Ph Dan Kekeruhan Menggunakan Metode Random Forest Berbasis Arduino,” *J. Pengemb. Teknol. Ilmu Komput.*, Vol. 9, No. 2, Pp. 2548–964, 2025.
- [27] T. D. A. N. Bentuk, “Algoritma Random Forest , Xgboost Dan Decision Tree Dengan Ekstraksi Fitur Algoritma Random Forest , Xgboost Dan Decision Tree Dengan Ekstraksi Fitur Dan Bentuk,” 2024.
- [28] F. B. P. Kusuma, D. B. Wibowo, And J. Prianggono, “Analisis Prediksi Tindak Pidana Pencurian Dengan Metode Klasifikasi Algoritma K-Nearest Neighbor Di Polresta Bengkulu, Polda Bengkulu,” *J. Portofolio J. Manaj.*

- Dan Bisnis*, Vol. 4, No. 1, Pp. 70–84, 2025, Doi: 10.70704/Jpjm.V4i1.354.
- [29] A. J. Binarto And A. Wibowo, “Implementasi Majority Voting Pada Framework Cross-Industry Standard Process For Data Mining Untuk Prediksi Kepatuhan Wajib Pajak,” 2025, Doi: 10.33364/Algoritma/V.22-1.2165.
- [30] U. Kannengiesser And J. S. Gero, “Modelling The Design Of Models: An Example Using Crisp-Dm,” *Proc. Des. Soc.*, Vol. 3, No. July, Pp. 2705–2714, 2023, Doi: 10.1017/Pds.2023.271.
- [31] M. A. Basiri, M. Parvin, And Z. Sobhani, “Implementing Crisp-Dm And Logistic Regression For Predictive Analysis In Financial Transactions : A Case Study Annual Conference On Information Systems Implementing Crisp-Dm And Logistic Regression,” 2024.
- [32] D. Fernando And R. G. Guntara, “Model Klasifikasi Penyebab Turnover Karyawan Menggunakan Kerangka Kerja Crisp-Dm,” No. 204, Pp. 383–392, 2022.
- [33] Y. W, R. Anto, D. Teguh Yuwono, And Y. Yuliadi, “Deteksi Serangan Vulnerability Pada Open Jurnal System Menggunakan Metode Black-Box,” *J. Inform. Dan Rekayasa Elektron.*, Vol. 4, No. 1, Pp. 68–77, 2021, Doi: 10.36595/Jire.V4i1.365.
- [34] M. P. A. Ginting And A. S. Lubis, “Pengujian Aplikasi Berbasis Web Data Ska Menggunakan Metode Black Box Testing,” *Cosm. J. Tek.*, Vol. 2, No. 1, Pp. 41–48, 2024, [Online]. Available: [Http://Creativecommons.Org/Licenses/By-Sa/4.0/](http://creativecommons.org/licenses/by-sa/4.0/)

- [35] A. Maspupah, "Literature Review: Advantages And Disadvantages Of Black Box And White Box Testing Methods," *Lchw*, Vol. 21, No. 2, 2022, [Online]. Available: <https://www.howandwhat.net/advantages-disadvantages-literature-review/>
- [36] A. C. Pamungkas And R. Samihardjo, "Evaluation Of The Utilization Of Web-Based Library Application Information Systems Using Whitebox And Blackbox Testing Methods," Vol. 7, No. 2, Pp. 17–24, 2024, Doi: 10.15408/Aism.V7i2.38876.

