

DAFTAR PUSTAKA

- [1] W. Andewi, S. Sucipto, E. Y. A, L. Anggraeni, and Z. Revita, "Pendampingan penggunaan teknologi informasi sebagai media pendukung optimalisasi pembelajaran daring tingkat sekolah dasar di PekonTotokarto," *NEAR Jurnal Pengabdian kepada Masyarakat*, vol. 1, no. 2, pp. 74–79, 5 2022. [Online]. Available: <https://doi.org/10.32877/nr.v1i2.428>
- [2] C. A. Cholik, "Perkembangan Teknologi Informasi Komunikasi / ICT dalam Berbagai Bidang," *Jurnal Fakultas Teknik UNISA Kuningan*, vol. 2, no. 2, pp. 39–46, 2021.
- [3] M. Rahul, "PENGEMBANGAN APLIKASI DETEKSI PHISING BERBASIS WEB MENGGUNAKAN ALGORITMA DECISION TREE," 2023.
- [4] A. Syahli, R. Kurniati, and N. Hidayasari, "Alat OSINT Berbasis Web untuk Deteksi URL Phishing Menggunakan Integrasi API," *Techno Com*, vol. 24, no. 3, pp. 905–918, 8 2025. [Online]. Available: <https://publikasi.dinus.ac.id/index.php/technoc/article/view/13769>
- [5] P. S. Hasugian, "PERANCANGAN WEBSITE SEBAGAI MEDIA PROMOSI DAN INFORMASI," vol. 3, no. 1, 2018.
- [6] A. S. Y. Irawan, N. Heryana, H. S. Hopipah, and D. Rahma, "Identifikasi Website Phishing dengan Perbandingan Algoritma Klasifikasi," *Syntax Jurnal Informatika*, vol. 10, no. 01, pp. 57–67, 6 2021. [Online]. Available: <https://journal.unsika.ac.id/index.php/syntax/article/view/5292>
- [7] F. S. S. Nagalay, "ANALISIS PENERAPAN ALGORITMA DECISION TREE DALAM KEAMANAN SIBER UNTUK KELASIFIKASI SITUS WEBSITE PHISHING," vol. 10, no. 1, 2024.
- [8] N. B. Putri and A. W. Wijayanto, "Analisis Komparasi Algoritma Klasifikasi Data Mining Dalam Klasifikasi Website Phishing," *Komputika : Jurnal Sistem Komputer*, vol. 11, no. 1, pp. 59–66, Jan. 2022. [Online]. Available: <https://ojs.unikom.ac.id/index.php/komputika/article/view/4350>
- [9] F. Purwiantono and A. Tjahyanto, "Model klasifikasi untuk deteksi situs phising di indonesia," 11 2017.
- [10] A. Nofiyah and M. Mushlihudin, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST)," *JSTIE (Jurnal Sarjana Teknik Informatika) (E-Journal)*, vol. 8, no. 2, p. 53, Jun. 2020. [Online]. Available: <http://journal.uad.ac.id/index.php/JSTIF/article/view/16697>

- [11] Yusrina, "Klasifikasi website phishing menggunakan algoritma random forest dengan teknik random oversampling," Majene, 2025, fakultas Teknik, Program Studi Informatika.
- [12] Indonesia Anti-Phishing Data Exchange (IDADX), "Laporan aktivitas phishing domain .id: Periode q4 2023," Pengelola Nama Domain Internet Indonesia (PANDI), Laporan Aktivitas Phishing, 2023.
- [13] R. P. Ramadhan and T. Desyani, "Implementasi Algoritma J48 Untuk Identifikasi Website," *Jurnal Ilmu Komputer*, vol. 1, no. 2, 2023.
- [14] L. Breiman, "Random forests," 2001, technical Report, Statistics Department, University of California, Berkeley. [Online]. Available: <https://www.stat.berkeley.edu/~breiman/randomforest2001.pdf>
- [15] A. A. Albishri *et al.*, "A comparative analysis of machine learning techniques for url phishing detection," *Engineering, Technology & Applied Science Research*, 2024. [Online]. Available: <https://etasr.com/index.php/ETASR/article/view/8920>
- [16] S. K. Lutfi Gani Al Achmad, *Website dan HTML*, 1st ed., ser. MSIM4309. Universitas Terbuka, 2020, no. Modul 01.
- [17] T. Berners-Lee, R. Cailliau, A. Luotonen, H. F. Nielsen, and A. Secret, *The World-Wide web*, 7 2023. [Online]. Available: <https://doi.org/10.1145/3591366.3591373>
- [18] Q. A. Al-Haija and M. Al-Fayoumi, "An intelligent identification and classification system for malicious uniform resource locators (URLs)," *Neural Computing and Applications*, vol. 35, no. 23, pp. 16 995–17 011, 4 2023. [Online]. Available: <https://doi.org/10.1007/s00521-023-08592-z>
- [19] I. C. Utomo and S. Rokhmah, "Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta," *Jurnal Rekayasa Teknologi Informasi (JURTI)*, vol. 6, no. 2, p. 143, 12 2022. [Online]. Available: <https://doi.org/10.30872/jurti.v6i2.8333>
- [20] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, p. 100031, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2772918423000188>
- [21] A. H. H. Harahap, C. D. Andani, A. Christie, D. Nurhaliza, and A. Fauzi, "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder," *Jurnal Manajemen dan Pemasaran Digital*, vol. 1, no. 2, pp. 73–83, 4 2023. [Online]. Available: <https://doi.org/10.38035/jmpd.v1i2.34>

- [22] A. Hermawan, T. Hartati, and Y. Wijaya, "Analisa keamanan data melalui website zahra software menggunakan metode keamanan informasi cia triad," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 7, pp. 125–130, 09 2022.
- [23] D. Ghelani, "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review," Sep. 2022. [Online]. Available: <https://www.authorea.com/users/506161/articles/587239-cyber-security-cyber-threats-implications-and-future-perspectives-a-review?commit=c6ec32c81c8730d72ed84cd70b010d9e817c6417>
- [24] M. A. Hama Saeed, "Malware in Computer Systems: Problems and Solutions," *IJID (International Journal on Informatics for Development)*, vol. 9, no. 1, p. 1, Apr. 2020. [Online]. Available: <http://ejournal.uin-suka.ac.id/saintek/ijid/article/view/1778>
- [25] V. F. Putra Y, "Modus operandi tindak pidana phishing menurut uu ite," *Jurist-Diction*, vol. 4, no. 6, pp. 2525–2548, November 2021. [Online]. Available: <https://e-journal.unair.ac.id/JD>
- [26] D. Rahmawati, M. Viendyasari, G. Lumakto, R. Kholifatur, W. Anindhita, R. Ameliah, S. Bachna, and A. Adienda, *Waspada Kejahatan Phishing Attack!*, cetakan i ed. Malang, Indonesia: PT. Literasi Nusantara Abadi Grup, May 2024, perancang sampul: Hasanuddin; Penata letak: Dicky Gea Nuansa. [Online]. Available: <https://www.penerbitlitnus.co.id>
- [27] F. D. Silalahi, *Keamanan Siber (Cyber Security)*, J. T. Santoso, Ed. Semarang: Yayasan Prima Agus Teknik, 2022, bekerja sama dengan Universitas Sains Teknologi Komputer (Universitas STEKOM).
- [28] A. Trianurahmah, A. Fauzi, E. N. Tyas, M. A. Suryanto, M. Rizky, and P. Wibisono, "Analisis ancaman pishing melalui aplikasi whatsapp: Studi kasus manajemen sekuriti waspadai maraknya kejahatan phishing dengan modus berbasis link," *ORBIT*, vol. 1, no. 2, pp. 60–74, Dec. 2024. [Online]. Available: <https://doi.org/10.63217/orbit.v1i2.81>
- [29] A. D. Prasetyo, H. B. Seta, and I. W. W. Pradnyana, "Analisis digital forensik Spear phishing menggunakan metode National Institute of Justice (Studi kasus: Instagram Verified Account)," *Informatik Jurnal Ilmu Komputer*, vol. 19, no. 1, pp. 58–67, 5 2023. [Online]. Available: <https://doi.org/10.52958/iftk.v19i1.4675>
- [30] BMKG-CSIRT. (2025) Jenis-jenis phishing, manakah yang berbahaya? BMKG-CSIRT. Jakarta, Indonesia. [Online]. Available: <https://csirt.bmkg.go.id/post/detail/jenis-jenis-phishing-manakah-yang-berbahaya>
- [31] M. Muharam and A. G. Persada, "Implementasi Penggunaan Website Sebagai Media Informasi dan Media Pemasaran Hasil Pertanian dan Peternakan Desa Sumberejo."

- [32] M. Sánchez-Paniagua, E. Fidalgo, V. González-Castro, and E. Alegre, "Impact of Current Phishing Strategies in Machine Learning Models for Phishing Detection," in *13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020)*, Herrero, C. Cambra, D. Urda, J. Sedano, H. Quintián, and E. Corchado, Eds. Cham: Springer International Publishing, 2021, vol. 1267, pp. 87–96, series Title: Advances in Intelligent Systems and Computing. [Online]. Available: http://link.springer.com/10.1007/978-3-030-57805-3_9
- [33] S. Marchal, G. Armano, T. Grondahl, K. Saari, N. Singh, and N. Asokan, "Off-the-Hook: an efficient and usable Client-Side phishing prevention application," *IEEE Transactions on Computers*, vol. 66, no. 10, pp. 1717–1733, 5 2017. [Online]. Available: <https://doi.org/10.1109/tc.2017.2703808>
- [34] R. G. Wardhana, G. Wang, and F. Sibuea, "PENERAPAN MACHINE LEARNING DALAM PREDIKSI TINGKAT KASUS PENYAKIT DI INDONESIA," *Journal of Information System Management (JOISM)*, vol. 5, no. 1, pp. 40–45, Jul. 2023. [Online]. Available: <https://jurnal.amikom.ac.id/index.php/joism/article/view/1136>
- [35] I. H. Sarker, "Machine learning: algorithms, real-world applications and research directions," *SN Computer Science*, vol. 2, no. 3, Mar. 2021. [Online]. Available: <https://pubmed.ncbi.nlm.nih.gov/33778771/>
- [36] 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, 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1319157823000034>
- [37] G. M. Toche Tchio, J. Kenfack, D. Kassegne, F.-D. Menga, and S. S. Ouro-Djobo, "A comprehensive review of supervised learning algorithms for the diagnosis of photovoltaic systems, proposing a new approach using an ensemble learning algorithm," *Applied Sciences*, vol. 14, no. 5, 2024. [Online]. Available: <https://www.mdpi.com/2076-3417/14/5/2072>
- [38] L. M. Cendani and A. Wibowo, "Perbandingan metode ensemble learning pada klasifikasi penyakit diabetes," *Jurnal Masyarakat Informatika*, vol. 13, no. 1, pp. 33–44, 2022.
- [39] R. E. Putri, Suparti, and R. Rahmawati, "Perbandingan metode klasifikasi naïve bayes dan k-nearest neighbor pada analisis data status kerja di kabupaten demak tahun 2012," *Jurnal Gaussian*, vol. 3, no. 4, pp. 831–838, oct 2014, universitas Diponegoro. [Online]. Available: <https://ejournal3.undip.ac.id/index.php/gaussian/article/view/8094>
- [40] L. Hakim, A. Sobri, L. Sunardi, and D. Nurdiansyah, "Prediksi penyakit jantung berbasis mesin learning dengan menggunakan metode k-nn," *Jurnal*

Digital Teknologi Informasi, vol. 7, no. 2, p. 14, Feb. 2025. [Online]. Available: <https://jurnal.um-palembang.ac.id/digital/article/view/9429>

- [41] Meta S. Brown, “Crisp-dm: Pengantar dan tahapan proses data mining,” CRISP-Data-Mining.pdf, 2014, dokumen terjemahan dan adaptasi dari buku *Data Mining for Dummies* oleh Meta S. Brown.
- [42] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 3rd ed. Cambridge, MA: MIT Press, 2009, p. 5.
- [43] S. Anggreani and Yahfizham, “Pengantar dan pengenalan konsep dasar algoritma pemrograman,” *Jurnal Pendidikan Berkarakter*, vol. 2, no. 1, pp. 282–294, Feb. 2024, e-ISSN: 2988-1129; p-ISSN: 2988-0661.
- [44] H. Blockeel, L. Devos, B. Frénay, G. Nanack, and S. Nijssen, “Decision trees: From efficient prediction to responsible ai,” *Frontiers in Artificial Intelligence*, vol. 6, p. 1124553, 2023. [Online]. Available: <https://doi.org/10.3389/frai.2023.1124553>
- [45] R. N. Ramadhon, A. Ogi, A. P. Agung, R. Putra, S. S. Febrihartina, and U. Firdaus, “Implementasi algoritma decision tree untuk klasifikasi pelanggan aktif atau tidak aktif pada data bank,” *Karimah Tauhid*, vol. 3, no. 2, pp. 1860–1874, 2024.
- [46] S. Amaliah, M. Nusrang, and Aswi, “Penerapan metode random forest untuk klasifikasi varian minuman kopi di kedai kopi konijwa bantaeng,” *VARIANSI: Journal of Statistics and Its Application on Teaching and Research*, vol. 4, no. 2, pp. 121–127, 2022.
- [47] R. Supriyadi, W. Gata, N. Maulidah, and A. Fauzi, “Penerapan algoritma random forest untuk menentukan kualitas anggur merah,” *Jurnal Ilmiah Ekonomi dan Bisnis*, vol. 13, no. 2, pp. 67–75, 2020. [Online]. Available: <http://journal.stekom.ac.id/index.php/E-Bisnis>
- [48] S. Maesaroh, A. Afyati, M. Yusuf, and E. B. Perkasa, *Bahasa Pemrograman Python*. Sada Kurnia Pustaka, 2024. [Online]. Available: https://www.researchgate.net/publication/381376588_Bahasa_Pemrograman_Python
- [49] Coursera. (2023) What is kaggle and what is it used for? [Accessed: 24-Oct-2025]. [Online]. Available: <https://www.coursera.org/articles/kaggle>
- [50] A. Rizky, “Pemanfaatan platform kaggle dalam pembelajaran data science dan machine learning,” *ResearchGate Preprint*, 2023, [Accessed: 24-Oct-2025]. [Online]. Available: https://www.researchgate.net/publication/373920563_Pemanfaatan_Platform_Kaggle_dalam_Pembelajaran_Data_Science_dan_Machine_Learning

- [51] T. Carneiro, R. V. M. da Nóbrega, T. Nepomuceno, G.-B. Bian, V. H. C. de Albuquerque, and P. P. R. Filho, "Performance analysis of google colab as a tool for accelerating deep learning applications," *IEEE Access*, vol. 6, pp. 61 677–61 684, 2018. [Online]. Available: <https://ieeexplore.ieee.org/document/8482685>
- [52] L. A. Dewi, A. J. Arifin, and A. Wibowo, "Perbandingan google colab dan google spreadsheet dalam menyelesaikan persamaan nonlinear metode bagi dua," *SCIENCE: Jurnal Inovasi Pendidikan Matematika dan IPA*, vol. 5, no. 3, pp. 1169–1177, 2025. [Online]. Available: <https://jurnalp4i.com/index.php/science>
- [53] 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, p. 8842, May 2022. [Online]. Available: <https://www.nature.com/articles/s41598-022-10841-5>
- [54] R. Yang, K. Zheng, B. Wu, C. Wu, and X. Wang, "Phishing Website Detection Based on Deep Convolutional Neural Network and Random Forest Ensemble Learning," *Sensors*, vol. 21, no. 24, p. 8281, Dec. 2021. [Online]. Available: <https://www.mdpi.com/1424-8220/21/24/8281>
- [55] M. R. Fatiha, I. Setiawan, A. N. Ikhsan, and I. R. Yunita, "OPTIMISASI SISTEM DETEKSI PHISHING BERBASIS WEB MENGGUNAKAN ALGORITMA DECISION TREE," *Jurnal Ilmiah IT CIDA*, vol. 10, no. 2, p. 97, Dec. 2024. [Online]. Available: <https://journal.amikomsolo.ac.id/index.php/itcida/article/view/212>
- [56] N. Bari, T. Saleem, M. Shah, A. Algarni, A. Patel, and I. Ullah, "A Filter-Based Feature Selection Framework to Detect Phishing URLs Using Stacking Ensemble Machine Learning," *CMES - Computer Modeling in Engineering and Sciences*, vol. 145, no. 1, pp. 1167–1187, 2025. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1526149225003716>
- [57] S. Work, "Web Page Phishing Detection Dataset," 2020, kaggle Dataset, accessed 2025-XX-XX. [Online]. Available: <https://www.kaggle.com/datasets/shashwatwork/web-page-phishing-detection-dataset>