

DAFTAR PUSTAKA

- [1] 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.
- [2] I. Suharjo and P. Wahyu Setyaningsih, "Identifikasi Dan Analisis Terjadinya Peretasan Pada Domain Website dari Data Google Cache," *Teknologi*, vol. 14, no. 1, pp. 61–70, May 2024, doi: 10.26594/teknologi.v14i1.4311.
- [3] N. A. ALfouzan and N. C, "A Systematic Approach for Malware URL Recognition," in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, IEEE, Jan. 2022, pp. 325–329. doi: 10.1109/ICCIT52419.2022.9711614.
- [4] Y. Risyani, S. Japit, C. Bombongan, T. Selamat, and Y. Yuliana, "Sistem Keamanan Siber Adaptif Berbasis AI: Analisis Kinerja, Arsitektur, dan Penerapannya pada Organisasi Modern," *Jurnal Minfo Polgan*, vol. 14, no. 2, pp. 2999–3006, Nov. 2025, doi: 10.33395/jmp.v14i2.15630.
- [5] R. Fauzan, A. V. Vitianingsih, D. Cahyono, A. L. Maukar, and Y. A. B. Suprio, "Penerapan Algoritma Klasifikasi pada Machine Learning untuk Deteksi Phishing," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 2, pp. 531–540, Mar. 2025, doi: 10.57152/malcom.v5i2.1968.
- [6] S. S. Maulina Putri, M. Arhami, and H. Hendrawaty, "Penerapan Metode SVM pada Klasifikasi Kualitas Air," *Journal of Artificial Intelligence and Software Engineering (J-AISE)*, vol. 3, no. 2, p. 93, Nov. 2023, doi: 10.30811/jaise.v3i2.4630.
- [7] N. Kamilatutsaniya, E. Daniati, and M. N. Muzaki, "Pemodelan Klasifikasi Popularitas Produk Skincare Menggunakan Support Vector Machine (SVM): Studi Komparatif Kinerja Kernel.," *The Indonesian Journal of Computer Science Research*, vol. 4, no. 2, pp. 86–95, Jul. 2025, doi: 10.59095/ijcsr.v4i2.209.
- [8] I. Pamungkas, S. Sumadi, and S. Alam, "Studi Komparasi Fungsi Aktivasi Sigmoid Biner, Sigmoid Bipolar dan Linear pada Jaringan Saraf Tiruan dalam Menentukan Warna RGB Menggunakan Matlab," *Jurnal Serambi Engineering*, vol. 7, no. 4, Oct. 2022, doi: 10.32672/jse.v7i4.4776.

- [9] A. Aljofey *et al.*, “An effective detection approach for phishing websites using URL and HTML features,” *Sci. Rep.*, vol. 12, no. 1, Dec. 2022, doi: 10.1038/s41598-022-10841-5.
- [10] A. Pradana and S. Susanto, “Implementasi Model Machine Learning untuk Deteksi Phishing 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.
- [11] 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, Dec. 2024, doi: 10.1038/s41598-024-74725-6.
- [12] R. N. F. Tanjung and S. Rahman, “Meningkatkan Deteksi Email Phising Melalui Pendekatan SVM yang Dioptimalkan NLP,” *INCODING: Journal of Informatics and Computer Science Engineering*, vol. 5, no. 1, pp. 38–50, Apr. 2025, doi: 10.34007/incoding.v5i1.831.
- [13] A. E. Karyawati, K. D. Y. Wijaya, I. W. Supriana, and I. W. Supriana, “A Comparison Of Different Kernel Functions Of SVM Classification Method For Spam Detection,” *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, vol. 8, no. 2, pp. 91–97, Feb. 2023, doi: 10.33480/jitk.v8i2.2463.
- [14] P. Fremmuzar and A. Baita, “Uji Kernel SVM dalam Analisis Sentimen Terhadap Layanan Telkomsel di Media Sosial Twitter,” *Komputika: Jurnal Sistem Komputer*, vol. 12, no. 2, pp. 57–66, Sep. 2023, doi: 10.34010/komputika.v12i2.9460.
- [15] B. D. Hartanto, T. A. Nugraha, B. R. Ramadhan, M. A. Pratama, and R. P. Alamsyah, “Edukasi Keamanan Digital untuk Meningkatkan Kewaspadaan Masyarakat Terhadap Link Phising,” *Jurnal Pengabdian Sosial*, vol. 2, no. 9, pp. 4341–4346, Jul. 2025, doi: 10.59837/nndaqp49.
- [16] S. Wahyuni, I. M. Raazi, and I. Dwitawati, “Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit,” *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 5, no. 1, pp. 49–55, Feb. 2022, doi: 10.32672/jnkti.v5i1.3962.

- [17] A. Muftiadi, T. P. M. Agustina, and M. Evi, "Studi kasus keamanan jaringan komputer: analisis ancaman phishing terhadap layanan online banking," *Hexatech: Jurnal Ilmiah Teknik*, vol. 1, no. 2, pp. 60–65, Aug. 2022, doi: 10.55904/hexatech.v1i2.346.
- [18] D. Patil, T. Pattewar, S. Pardeshi, V. Punjabi, and R. Wagh, "Learning to Detect Phishing Web Pages Using Lexical and String Complexity Analysis," *ICST Transactions on Scalable Information Systems*, p. 173950, Jul. 2022, doi: 10.4108/eai.20-4-2022.173950.
- [19] S. S. Peter, G. P, D. A, and A. N, "Adversarially-Hardened URL Classification Pipeline: Hybrid Lexical-Structural Analysis with Sparse Matrix-Optimized Logistic Regression for Real-Time Threat Mitigation," in *2025 First International Conference of Advances in Engineering and Computing Technologies for Sustainable Development (AECTSD)*, IEEE, Dec. 2025, pp. 1–7. doi: 10.1109/AECTSD65988.2025.11411045.
- [20] H. Eldo, A. Ayuliana, D. Suryadi, G. Chrisnawati, and L. Judijanto, "Penggunaan Algoritma Support Vector Machine (SVM) Untuk Deteksi Penipuan pada Transaksi Online," *Jurnal Minfo Polgan*, vol. 13, no. 2, pp. 1627–1632, Oct. 2024, doi: 10.33395/jmp.v13i2.14186.
- [21] V. Indraini, H. Listiyono, and S. Saefurrahman, "Deteksi Phishing Website Menggunakan Support Vector Machine, Gradient Boosting, dan Neural Networks," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 2, pp. 3107–3113, Apr. 2025, doi: 10.36040/jati.v9i2.13214.
- [22] T. Z. Jasman, E. Hasmin, Sunardi, C. Susanto, and W. Musu, "Perbandingan Logistic Regression, Random Forest, dan Perceptron pada Klasifikasi Pasien Gagal Jantung," *CSRID (Computer Science Research and Its Development Journal)*, vol. 14, no. 3, pp. 271–286, Dec. 2022, doi: 10.22303/csrid-.14.3.2022.271-286.
- [23] L. Pebrianti, E. Simamora, S. Manullang, I. Taufiq, and C. Chairunisah, "Perbandingan Metode Algoritma Supervised Naive Bayes Dan Support Vector Machine (SVM) Dalam Klasifikasi Penderita Stunting Di Kabupaten Deli Serdang," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 3, pp. 4327–4333, May 2025, doi: 10.36040/jati.v9i3.13649.

- [24] N. H. Ovirianti, M. Zarlis, and H. Mawengkang, "Support Vector Machine Using A Classification Algorithm," *Sinkron*, vol. 7, no. 3, pp. 2103–2107, Aug. 2022, doi: 10.33395/sinkron.v7i3.11597.
- [25] A. A. Jadhav and P. S. Pisal, "Harnessing Kernel Tricks for Nonlinear Problem Solving: SVM Applications," in *2025 5th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, IEEE, May 2025, pp. 1–7. doi: 10.1109/IRASET64571.2025.11007960.
- [26] S. Saifuddin, L. Azhari, E. Widarti, and W. Wartono, "Evaluasi Kinerja Kernel Linear, RBF, dan Polynomial pada Model Support Vector Machine untuk Prediksi Risiko Hipertensi," *Jurnal Ilmiah FIFO*, vol. 17, no. 2, p. 192, Nov. 2025, doi: 10.22441/fifo.2025.v17i2.008.
- [27] S. S. Wijayanti, E. Utami, and A. Yaqin, "Comparison of Kernels on Support Vector Machine (SVM) Methods for Analysis of Cyberbullying," in *2022 6th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, IEEE, Dec. 2022, pp. 104–108. doi: 10.1109/ICITISEE57756.2022.10057761.
- [28] F. S. Gomiasti, W. Wardo, E. Kartikadarma, J. Gondohanindijo, and D. R. I. M. Setiadi, "Enhancing Lung Cancer Classification Effectiveness Through Hyperparameter-Tuned Support Vector Machine," *Journal of Computing Theories and Applications*, vol. 1, no. 4, pp. 396–406, Mar. 2024, doi: 10.62411/jcta.10106.
- [29] F. Pritama, Ekat Rueh Daya Leluni, Yovita, and Jadianan Parhusip, "Analisis Distribusi Kinerja SVM dan KNN Berdasarkan Rata Rata Simpangan Baku dan Stabilitas," *Informatech : Jurnal Ilmiah Informatika dan Komputer*, vol. 1, no. 2, Dec. 2024, doi: 10.69533/xgqngy78.
- [30] W. Wijiyanto, A. I. Pradana, S. Sopingi, and V. Atina, "Teknik K-Fold Cross Validation untuk Mengevaluasi Kinerja Mahasiswa," *Jurnal Algoritma*, vol. 21, no. 1, May 2024, doi: 10.33364/algoritma/v.21-1.1618.
- [31] F. Pritama, Ekat Rueh Daya Leluni, Yovita, and Jadianan Parhusip, "Analisis Distribusi Kinerja SVM dan KNN Berdasarkan Rata Rata Simpangan Baku dan Stabilitas," *Informatech : Jurnal Ilmiah Informatika dan Komputer*, vol. 1, no. 2, Dec. 2024, doi: 10.69533/xgqngy78.

- [32] D. Valero-Carreras, J. Alcaraz, and M. Landete, "Comparing two SVM models through different metrics based on the confusion matrix," *Comput. Oper. Res.*, vol. 152, p. 106131, Apr. 2023, doi: 10.1016/j.cor.2022.106131.
- [33] F. Fatmawati, R. Sunartaty, and F. Meutia, "Validasi metode pengujian kadar air dengan analisis perbandingan akurasi dan presisi," *Serambi Journal of Agricultural Technology*, vol. 5, no. 1, Jun. 2023, doi: 10.32672/sjat.v5i1.6214.
- [34] M. Fahri, "Penerapan Algoritma Random Forest untuk Deteksi Phishing pada Website," *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 2, pp. 186–194, Jun. 2025, doi: 10.62527/jitsi.6.2.472.
- [35] Marissa Utami and E. D. Putra, "Metode Identifikasi Pengenalan Wajah Menggunakan Metode Haar Feature," *JSAT (Journal Scientific and Applied Informatics)*, vol. 6, no. 3, pp. 457–461, Nov. 2023, doi: 10.36085/jsai.v6i3.4997.
- [36] F. T. Admojo and Y. I. Sulistya, "Analisis Performa Algoritma Stochastic Gradient Descent (SGD) Dalam Mengklasifikasi Tahu Berformalin," *Indonesian Journal of Data and Science*, vol. 3, no. 1, pp. 1–8, Mar. 2022, doi: 10.56705/ijodas.v3i1.42.
- [37] 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," in *Proceedings of the 11th International Conference on Networking, Systems, and Security*, New York, NY, USA: ACM, Dec. 2024, pp. 137–145. doi: 10.1145/3704522.3704532.
- [38] I. Altan, A. Bachir, Y. Parbhulkar, A. M. Rizvi, and M. Farazi, "Dual-Path Phishing Detection: Integrating Transformer-Based NLP with Structural URL Analysis," Sep. 2025, [Online]. Available: <http://arxiv.org/abs/2509.20972>
- [39] P. von Stackelberg, R. Goedhart, Ş. İ. Birbil, and R. J. M. M. Does, "Comparison of threshold tuning methods for predictive monitoring," *Qual. Reliab. Eng. Int.*, vol. 40, no. 1, pp. 499–512, Feb. 2024, doi: 10.1002/qre.3436.
- [40] D. Patil, T. Pattewar, S. Pardeshi, V. Punjabi, and R. Wagh, "Learning to Detect Phishing Web Pages Using Lexical and String Complexity Analysis," *ICST Transactions on Scalable Information Systems*, p. 173950, Jul. 2018, doi: 10.4108/eai.20-4-2022.173950.

- [41] A. Aljofey *et al.*, “An effective detection approach for phishing websites using URL and HTML features,” *Sci. Rep.*, vol. 12, no. 1, Dec. 2022, doi: 10.1038/s41598-022-10841-5.
- [42] S. S. Peter, G. P, D. A, and A. N, “Adversarially-Hardened URL Classification Pipeline: Hybrid Lexical-Structural Analysis with Sparse Matrix-Optimized Logistic Regression for Real-Time Threat Mitigation,” in *2025 First International Conference of Advances in Engineering and Computing Technologies for Sustainable Development (AECTSD)*, IEEE, Dec. 2025, pp. 1–7. doi: 10.1109/AECTSD65988.2025.11411045.

