

DAFTAR PUSTAKA

- Alam, M. N., Sarma, D., Lima, F. F., Saha, I., Ulfath, R. E., & Hossain, S. (2020). Phishing Attacks Detection using Machine Learning Approach. *Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT* 2020, 1173–1179. <https://doi.org/10.1109/ICSSIT48917.2020.9214225>
- Aldakheel, E. A., Zakariah, M., Gashgari, G. A., Almarshad, F. A., & Alzahrani, A. I. A. (2023). A Deep Learning-Based Innovative Technique for Phishing Detection in Modern Security with Uniform Resource Locators. *Sensors*, 23(9), 4403. <https://doi.org/10.3390/s23094403>
- Alfawaid, M. F., & Prianggono, J. (2023). Penerapan Metode Multiple Machine Learning (Hybrid Model) Untuk Mendeteksi Link Phishing Sebagai Upaya Preventif Dalam Meminimalisir Korban Pencurian Data. *Jurnal Ilmu Kepolisian*, 17(3).
- Aljammal, A. H., Taamneh, S., Qawasmeh, A., & Salameh, H. B. (2023). Machine Learning Based Phishing Attacks Detection Using Multiple Datasets. *International Journal of Interactive Mobile Technologies*, 17(5), 71–83. <https://doi.org/10.3991/ijim.v17i05.37575>
- Amriza, R. N. S., & Supriyadi, D. (2021). Komparasi Metode Machine Learning dan Deep Learning untuk Deteksi Emosi pada Text di Sosial Media. *Jurnal JUPITER*, 13(2), 130–139.
- Andarsyah, R., & Yanuar, A. (2024). Sentimen Analisis Aplikasi Posaja Pada Google Playstore Untuk Peningkatan Pospay Superapp Menggunakan Support Vector Meachine. *Jurnal Teknik Informatika*, 16(2).
- Anti-Phishing Working Group (APWG). (2024). *Phishing Activity Trends Report 4rd Quarter 2024*. Retrieved from <http://www.apwg.org>,

- Brownlee, J. (2017). *Long Short-Term Memory Networks With Python Develop Sequence Prediction Models With Deep Learning*. Machine Learning Mastery.
- By Haqi, Moh. I. (2020). *Penerapan Chatbot Untuk Mendeteksi Kemiripan Gambar Asli Atau Manipulasi Menggunakan Metode Metadata Dan Error Level Analysis (Ela) Sebagai Komputasi Cnn*. Universitas Komputer Indonesia, Bandung.
- Daqiqi, I. I. (2021). *MACHINE LEARNING: Teori, Studi Kasus dan Implementasi Menggunakan Python*. Pekanbaru: UR PRESS.
- Defiyanti, S. (2016). Analisis dan Prediksi Kinerja Mahasiswa Menggunakan Teknik Data Mining. *Syntax: Jurnal Informatika*, 2(01). <https://doi.org/10.35706/syji.v2i01.192>
- Deisenroth, M. P., Faisal, A. A., & Ong, C. S. (2020). *Mathematics For Machine Learning*. Cambridge University Press. Retrieved from <https://mml-book.com>.
- Egigogo, A. R., Idris, I., Olalere, M., & Aderiike, A. O. (2024). Evaluating Deep Learning Models for Website Phishing Attack Detection: A Comparative Analysis. *Ceddi Journal of Information System and Technology (JST)*, 3(2), 19–29. <https://doi.org/10.56134/jst.v3i2.100>
- Farida, & Mustopa, A. (2023). Perbandingan Logistic Regression dan Random Forest menggunakan Correlation-based Feature Selection untuk Deteksi Website Phishing. *Jurnal Sistem Informasi*, 12(1), 13–20. Retrieved from <http://sistemasi.ftik.unisi.ac.id>
- Fatiha, M. R., Setiawan, I., Ikhsan, A. N., & Yunita, I. R. (2024). Optimisasi Sistem Deteksi Phishing Berbasis Web Menggunakan Algoritma Decision Tree. *Jurnal Ilmiah IT CIDA : Diseminasi Teknologi Informasi*, 10(2), 97–108. Retrieved from <https://www.kaggle.com>

- Frosa, B. Da, Zaini, A., & Tri, M. P. (2024). Investigasi Perbandingan Cosine Similarity Dan Euclidean Distance Dalam Deteksi Phishing Attack Menggunakan Metode K-Nearest Neighbor. *Jurnal Riset Mahasiswa Bidang Teknologi Informasi*, 6(2), 194–199. Retrieved from <https://ejournal.unikama.ac.id/index.php/JFTI>
- Ghifari, M. A. G. Al, Hananto, B., & Wahyono, B. T. (2022). Implementasi Ekstensi Google Chrome Dalam Mendeteksi Situs Web Phishing Menggunakan Algoritma Random Forest. *Seminar Nasional Mahasiswa Ilmu Komputer Dan Aplikasinya (SENAMIKA)*.
- Handoyo, T. F., & Putra, M. P. K. (2025). Optimasi Bobot Kelas LSTM untuk Deteksi URL Phishing pada Dataset Tidak Berimbang. *Jurnal Informatika: Jurnal Pengembangan IT*, 10(1), 20–36. <https://doi.org/10.30591/jpit.v10i1.8128>
- Hinton, G. E., Srivastava, N., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. R. (2012). *Improving neural networks by preventing co-adaptation of feature detectors*. Retrieved from <https://arxiv.org/abs/1207.0580v1>
- Kamila, A. R., Adikara, F., Sutrisno, & Herdian, C. (2024). Analisa Pengaruh Penambahan Fitur dengan Perbandingan Algoritma berbasis Bagging dan Boosting pada Deteksi Phishing Link. *JEPIN (Jurnal Edukasi Dan Penelitian Informatika)*, 10(3).
- Kingma, D. P., & Ba, J. (2015). *Adam: A Method for Stochastic Optimization*. Retrieved from <http://arxiv.org/abs/1412.6980>
- Liao, L., Li, H., Shang, W., & Ma, L. (2022). An Empirical Study of the Impact of Hyperparameter Tuning and Model Optimization on the Performance Properties of Deep Neural Networks. *ACM Transactions on Software Engineering and Methodology*, 31(3), 1–40. <https://doi.org/10.1145/3506695>

- Mahmud, A. F., & Wirawan, S. (2024). Deteksi Phishing Website menggunakan Machine Learning Metode Klasifikasi. *Sistemasi: Jurnal Sistem Informasi*, 13(4), 1368–1380. Retrieved from <http://sistemasi.ftik.unisi.ac.id>
- Meilina, K. (2025, March 26). WNA Cina Bobol Rekening Warga RI Pakai SMS Bank dan BTS Palsu, Begini Modusnya. *Katadata.Co.Id*.
- Moedjahedy, J. H., Setyanto, A., & Aryasa, K. (2020). Analisis Perbandingan Korelasi Spearman Dan Maximal Information Coefficient Dalam Seleksi Fitur Website Phishing Menggunakan Algoritma Machine Learning. *CSRID (Computer Science Research and Its Development Journal)*, 12(2), 107–116. <https://doi.org/10.22303/csrid.12.2.2020.107-116>
- Nanda, E., Istikomah, Amari, N. A., & Pristyanto, Y. (2018). Perbandingan Klasifikasi Algoritma K-Nn, Neural Network, Naïve Bayes, C 4.5 Untuk Mendeteksi Web Phising. *Fahma Jurnal Informatika Komputer, Bisnis Dan Managemen*, 16(3), 33–42. Retrieved from <https://archive.ics.uci.edu/ml/datasets/Website+Phishing>.
- Naufal, M. F., & Kusuma, S. F. (2023). Analisis Perbandingan Algoritma Machine Learning Dan Deep Learning Untuk Klasifikasi Citra Sistem Isyarat Bahasa Indonesia (SIBI). *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIK)*, 10(4), 873–882. <https://doi.org/10.25126/jtiik.2023106828>
- Nugraha, A. F., Aziza, R. F. A., & Pristyanto, Y. (2022). Penerapan Metode Stacking dan Random Forest untuk Meningkatkan Kinerja Klasifikasi pada Proses Deteksi Web Phishing. *Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan*, 7(1), 39–44.
- Pratama, B. O. (2024). *Analisis Sentimen Tempat Wisata Di Pulau Bintan Menggunakan Metode Support Vektor Machine (SVM)* (Skripsi). Universitas Maritim Raja Ali Haji, Tanjungpinang.

- Purwiantono, F. E. (2017). *Model Klasifikasi Untuk Deteksi Situs Phising Di Indonesia*. Institut Teknologi Sepuluh Nopember, Surabaya.
- Putri, N. B., & Wijayanto, A. W. (2022). Analisis Komparasi Algoritma Klasifikasi Data Mining Dalam Klasifikasi Website Phishing. *Komputika : Jurnal Sistem Komputer*, 11(1), 59–66. <https://doi.org/10.34010/komputika.v11i1.4350>
- Rad, J. A., Parand, K., & Chakraverty, S. (2023). *Learning with Fractional Orthogonal Kernel Classifiers in Support Vector Machines* (J. A. Rad, K. Parand, & S. Chakraverty, Eds.). Singapore: Springer Nature Singapore. <https://doi.org/10.1007/978-981-19-6553-1>
- Rahmadini, LorencisLubis, E. E., Priansyah, A., R.W.N, Y., & Meutia, T. (2023). Penerapan Data Mining Untuk Memprediksi Harga Bahan Pangan Di Indonesia Menggunakan Algoritma K-Nearest Neighbor. *Jurnal Mahasiswa Akuntansi Samudra*, 4(4), 223–235. <https://doi.org/10.33059/jmas.v4i4.7074>
- Rahman, O. H., Abdillah, G., & Komarudin, A. (2021). Klasifikasi Ujaran Kebencian pada Media Sosial Twitter Menggunakan Support Vector Machine. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 5(1), 17–23. <https://doi.org/10.29207/resti.v5i1.2700>
- Raihan, A., Fadhli, M., & Lindawati. (2024). IMPLEMENTATION OF DEEP LEARNING FOR DETECTING PHISHING ATTACKS ON WEBSITES WITH COMBINATION OF CNN AND LSTM. *Jurnal Teknik Informatika (JUTIF)*, 5(5), 1451–1459. <https://doi.org/10.52436/1.jutif.2024.5.5.2446>
- Raup, A., Ridwan, W., Khoeriyah, Y., Supiana, & Zaqiah, Q. Y. (2022). Deep Learning dan Penerapannya dalam Pembelajaran. *JiIP (Jurnal Ilmiah Ilmu Pendidikan)*, 5(9). Retrieved from <http://Jiip.stkipyapisdompu.ac.id>
- Reddy, V. V. K., Sai, Y. N., Keerthi, T., & Reddy, K. A. (2023). Detection of Phishing Website Using Support Vector Machine and Light Gradient

- Boosting Machine Learning Algorithms. *Lecture Notes in Networks and Systems*, 731, 297–308. https://doi.org/10.1007/978-981-99-4071-4_23
- Septian, A. D. (2018). *Skripsi SVM*. Universitas Brawijaya, Malang.
- Septiani, A. (2020). *Klasifikasi Penyakit Jantung Menggunakan Metode Recurrent Neural Network (RNN)*. Universitas Sriwijaya, Palembang.
- Setyawan, G. D., Yuswanto, A., Ridwan, A. M., Wibowo, B., & Firmansyah, M. (2023). Implementasi Metode Adasyn Dalam Deteksi Url Berbahaya Menggunakan Machine Learning: Demi Meningkatkan Keamanan Siber Di Era Digital. *TEKNOKOM: Jurnal Teknologi Dan Rekayasa Sistem Komputer*, 6(2), 123–126. <https://doi.org/10.31943/teknokom.v6i2.153>
- Sonowal, G. (2022). *Phishing and Communication Channels*. Berkeley, CA: Apress. <https://doi.org/10.1007/978-1-4842-7744-7>
- Soon, G. K., On, C. K., Rusli, N. M., Fun, T. S., Alfred, R., & Guan, T. T. (2020). Comparison of Simple Feedforward Neural Network, Recurrent Neural Network and Ensemble Neural Networks in Phishing Detection. *Journal of Physics: Conference Series*, 1502(1). <https://doi.org/10.1088/1742-6596/1502/1/012033>
- Syafia, A. N. (2024). *Implementasi Algoritma Long Short-Term Memory Pada Sistem Deteksi Situs Phishing Berbasis Aplikasi Web (Skripsi)*. Universitas Pendidikan Indonesia, Bandung.
- Syahrizal, M., & Haryati. (2018). Perancangan Aplikasi Sistem Pakar Deteksi Kerusakan Mesin Alat Berat (Beko) Dengan Menerapkan Metode Teorema Bayes. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 2(2). <https://doi.org/10.30865/mib.v2i2.596>
- Umam, A., & Santoso, B. (2018). *Data Mining dan Big Data Analytics* (2nd ed). Yogyakarta: Penebar Media Pustaka.

- Wahyudi, D. (2020). *Aplikasi Pendeteksi Website Phishing Menggunakan Machine Learning*. Universitas Hasanuddin, Makassar.
- Wahyudi, R., Marcos, H., Hasanah, U., Hartato, B. P., Astuti, T., & Prasetyo, R. A. (2018). Algorithm Evaluation for Classification “Phishing Website” Using Several Classification Algorithms. *(ICITISEE) International Conferences on Information Technology, Information Systems and Electrical Engineering*.
- Widodo, S. (2017). Klasifikasi Situs Phishing dengan Menggunakan Neural Network dan K-Nearest Neighbor. *INFORMATION MANAGEMENT FOR EDUCATORS AND PROFESSIONALS*, 1(2), 145–154.
- Windarni, V. A., Nugraha, A. F., Ramadhani, S. T. A., Istiqomah, D. A., Puri, F. M., & Setiawan, A. (2023). Deteksi Website Phishing Menggunakan Teknik Filter Pada Model Machine Learning. *Information System Journal (INFOS)*, 6(1), 39–43.
- Zhao, Z.-Q., Zheng, P., Xu, S.-T., & Wu, X. (2019). Object Detection With Deep Learning: A Review. *IEEE Transactions on Neural Networks and Learning Systems*, 30(11), 3212–3232. <https://doi.org/10.1109/TNNLS.2018.2876865>
- Zuhayr, N. A., Girinoto, Qomariasih, N., & Setiawan, H. (2023). Detection Model for URL Phishing with Comparison Between Shallow Machine Learning and Deep Learning Models. *Proceedings of the 1st International Conference on Neural Networks and Machine Learning 2022 (ICONNSMAL 2022)*, 146–156. Atlantis Press. https://doi.org/10.2991/978-94-6463-174-6_13