DAFTAR PUSTAKA

Adiputraa, O., & Setiawan, E. (2023). Klasifikasi Malicious URL Menggunakan Algoritma Improved Random Forest dan Random Forest Berbasis Web. *Jurnal Sains Dan Informatika*, *9*(1), 8–14. https://doi.org/10.22216/jsi.v9i1.1378

Atrees, M., Ahmad, A., & Alghanim, F. (2022). Enhancing detection of malicious urls using boosting and lexical features. *Intelligent Automation and Soft Computing*, *31*(3), 1405–1422. https://doi.org/10.32604/IASC.2022.020229

Aung, E. S., & Yamana, H. (2019, December 2). URL-based phishing detection using the entropy of non- A lphanumeric characters. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3366030.3366064

Cui, B., He, S., Yao, X., & Shi, P. (2018). Malicious URL detection with feature extraction based on machine learning. *Int. J. High Performance Computing and Networking*, *12*(2), 166–178.

Das, A., Das, A., Datta, A., Si, S., & Barman, S. (2020). *Deep Approaches on Malicious URL Classification*.

Fatni, Z. (2021). *Klasifikasi Citra Magnetic Resonance Imaging (Mri) Otak Dalam Mengidentifikasi Tumor Menggunakan Algoritma Random Forest*.

Gomes, H. M., Bifet, A., Read, J., Barddal, J. P., Enembreck, F., Pfharinger, B., Holmes, G., & Abdessalem, T. (2017). Adaptive random forests for evolving data stream classification. *Machine Learning*, *106*(9–10), 1469–1495. https://doi.org/10.1007/s10994-017-5642-8

Grandini, M., Bagli, E., & Visani, G. (2020). *Metrics for Multi-Class Classification: an Overview*. http://arxiv.org/abs/2008.05756

Haganta Depari, D., Widiastiwi, Y., Mega Santoni, M., Ilmu Komputer, F., Pembangunan Nasional Veteran Jakarta, U., Fatmawati Raya, J. R., & Labu, P. (n.d.). Perbandingan Model Decision Tree, Naive Bayes dan Random Forest untuk Prediksi Klasifikasi Penyakit Jantung. *JURNAL INFORMATIK Edisi Ke*, *18*, 2022.

Perdana, V. P., & Octavya, N. H. (2018). Identifikasi Malicious Web Menggunakan Metode Random Forest. *Prosiding Annual Research Seminar*.

Sahoo, D., Liu, C., & Ho, S. C. H. (2022). Malicious URL Detection using Machine Learning: A Survey. *IEEE International Conference on Program Comprehension*, *2022-March*, 36–47. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Sandag, G. A., Leopold, J., & Ong, V. F. (2018). Klasifikasi Malicious Websites Menggunakan Algoritma K-NN Berdasarkan Application Layers dan Network Characteristics. *Cogito Smart Journal*, *4*(1).

Suh, Y., Yu, J., Mo, J., Song, L., & Kim, C. (n.d.). *A Comparison of Oversampling Methods on Imbalanced Topic Classification of Korean News Articles*.

Syed, A. A. (2011). *Malicious URL Detection Using Machine Learning A Report Submitted in Partial Fulfilment of the Requirements for the Degree of MASTER OF ENGINEERING in the Department of Electrical and Computer Engineering*.

Telo, J. (2022). *Supervised Machine Learning for Detecting Malicious URLs: An Evaluation of Different Models*. https://orcid.org/0009-0004-5101-8064

Uçar, E. (2019). *A DEEP LEARNING APPROACH FOR DETECTION OF MALICIOUS URLS*. https://www.researchgate.net/publication/338477987

Valdis Tjahjadi, E., & Santoso, B. (2023). Klasifikasi Malware Menggunakan Teknik Machine Learning. *Jurnal Ilmiah Ilmu Komputer*, *2*(1). https://www.kaggle.com/datasets/amauricio/pe-files-malwares.

Wahid, A. A. (2020). Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi. *Jurnal Ilmu-Ilmu Informatika Dan Manajemen STMIK*.

Xuan, C. Do, Nguyen, H. D., & Nikolaevich, T. V. (2020). Malicious URL Detection based on Machine Learning. *IJACSA) International Journal of Advanced Computer Science and Applications*, *11*(1). www.ijacsa.thesai.org

Zabar, A. A., & Novianto, F. (2015). Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux. *Jurnal Ilmiah Komputer Dan Informatika (KOMPUTA)*, *69*(2).