DAFTAR PUSTAKA

Adenansi, R., & Novarina, L. A. (2017). Malware Dynamic.

Adiputra, 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.

Akhtar, M. S., & Feng, T. (2022). Malware Analysis and Detection Using Machine Learning Algorithms. *Symmetry*, *14*(11). https://doi.org/10.3390/sym14112304

Azzahra Nasution, D., Khotimah, H. H., & Chamidah, N. (2019). *Perbandingan Normalisasi Data Untuk Klasifikasi Wine Menggunakan Algoritma K-NN (Vol. 4, Nomor 1)*.

Damanik, R. A., Seta, H. B., & Theresiawati. (2023). *Analisis Trojan Dan Spyware Menggunakan Metode Hybrid Analysis*.

Garcia, S., Parmisano, A., & Erquiaga, M. J. (2020). *IoT-23: A labeled dataset with malicious and benign IoT network traffic*.

Hamdi, F. S., & Maita, I. (2022). Pelatihan Pembuatan Website Memanfaatkan Wix Untuk Blog Pribadi Pada Siswa SMAN 2 Gunung Talang. *CONSEN: Indonesian Journal of Community Services and Engagement*, *2*(2), 64–69. https://doi.org/10.57152/consen.v2i2.471

Hananta Firdaus, D., Imran, B., Darmawan Bakti, L., & Suryadi, E. (2022). Klasifikasi Penyakit Katarak Pada Mata Menggunakan Metode Convolutional Neural Network (CNN) Berbasis Web. Dalam *Jurnal Kecerdasan Buatan dan Teknologi Informasi (JKBTI)* (Vol. 1, Nomor 3).

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains dan Teknologi*, *2*(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

Kusumaningrum, T. F. (2018). Implementasi Convolution Neural Network (Cnn) Untuk Klasifikasi Jamur Konsumsi Di Indonesia Menggunakan Keras.

Lee, H., & Song, J. (2019). Introduction to convolutional neural network using Keras; An understanding from a statistician. *Communications for Statistical Applications and Methods*, *26*(6), 591–610. https://doi.org/10.29220/CSAM.2019.26.6.591

Liang, Y., & Vankayalapati, N. (2021). *Machine Learning and Deep learning Methods for Better Anomaly Detection in IoT-23 Dataset Cybersecurity*.

Libovický, J. (2017). *Deep learning for Natural Language processing Introduction to Natural Language Processing*.

Mahdi, F. A., Lukito, C. A., Parwita, D., Nofri, A., Madjid, V. A., & Prasvita, D. S. (2021). Pengaruh Principal Component Analysis terhadap Akurasi Model Machine Learning dengan Algoritma Artificial Neural Network untuk Prediksi Kebangkrutan Perusahaan. Dalam *Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA) Jakarta-Indonesia*.

Nurfauzi, N. A. (2022). *Deteksi Serangan Malware Pada Cloud Server Menggunakan Metode Anomaly Based*.

Putra, J. W. G. (2020). *Pengenalan Pembelajaran Mesin dan Deep learning*. 150–151.

Python. (2021). *Python FLask*.

Rangga, M., Nasution, A., & Hayaty, M. (2019). Perbandingan Akurasi dan Waktu Proses Algoritma K-NN dan SVM dalam Analisis Sentimen Twitter. *Jurnal Informatika*, *6*(2), 212–218. http://ejournal.bsi.ac.id/ejurnal/index.php/ji

Rizki, M., Basuki, S., & Azhar, Y. (2020). Implementasi *Deep learning* Menggunakan Arsitektur Long Short Term Memory Untuk Prediksi Curah Hujan Kota Malang. *REPOSITOR*, *2*(3), 331–338.

Sahu, A. K., Sharma, S., Tanveer, M., & Raja, R. (2021). Internet of Things attack detection using hybrid *Deep learning* Model. *Computer Communications*, *176*, 146–154. https://doi.org/10.1016/j.comcom.2021.05.024

Silviana, Kurniawan, R., Nazir, A., Budianita, E., Syarifa, F., & Gusti, K. S. (2022). *Pengklasteran Risiko Covid-19 Di Riau Menggunakan Teknik One Hot Encoding Dan Algoritma K-Means Clustering*.

Stoian, N.-A. (2020). *Machine Learning for Anomaly Detection in IoT networks: Malware analysis on the IoT-23 Data set*.

Suprayogi, C., & Marwan, M. A. (2022). Classification of Network Traffic Data Mirai *Malware* Attacks on Internet of Things Devices Using the K-Nearest Neighbor Method. *International Research Journal of Advanced Engineering and Science*, *7*(4), 39–43.