DAFTAR PUSTAKA

[1] G. Rahmadi, “Analisis Kesadaran Cyber Security pada Kalangan Pelaku e-Commerce di Indonesia,” 2019.

[2] A. Sandriana and F. Maulana, “Klasifikasi serangan Malware terhadap Lalu Lintas Jaringan Internet of Things menggunakan Algoritma K-Nearest Neighbour (K-NN),” vol. 03, no. 1, pp. 12–22, 2022.

[3] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, “Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis,” pp. 19–30.

[4] Z. Bazrafshan, H. Hashemi, S. Mehdi, H. Fard, and A. Hamzeh, “A Survey on Heuristic Malware Detection Techniques,” no. February 2018, 2019, doi: 10.1109/IKT.2013.6620049.

[5] S. Wo and A. Alm, “Review of Advances in Neural Networks : Neural Design Technology Stack,” vol. 1, pp. 367–368, 2014, doi: 10.1007/978-3-319-14063-6.

[6] D. T. Rachmadie, “REGULASI PENYIMPANGAN ARTIFICIAL INTELLIGENCE PADA TINDAK PIDANA MALWARE BERDASARKAN UNDANG-UDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2018,” vol. 9, no. 2, pp. 128–136, 2016.

[7] D. W. Asry, E. Siswanto, D. Kurniawan, and H. I. Huda, “Deteksi Malware Statis Menggunakan Deep Neural Networks Pada Portable Executable,” vol. 3, no. 1, pp. 19–34, 2023.

[8] J. Yan, “Detecting Malware with an Ensemble Method Based on Deep Neural Network,” vol. 2018, 2018.

[9] P. V. Sahni, “Malware Detection in Android platform using DNN Akshay Ashok Wakhare National College of Ireland Supervisor :”.

[10] F. Surahman, “Tantangan Dalam Menjaga Keamanan Data Official Statistics dari Serangan Cybercrime,” *J. Ilm. Multidisiplin*, vol. 1, no. 11, pp. 904–907, 2023, [Online]. Available: https://doi.org/10.5281/zenodo.10371686

[11] D. Mualfah, “Forensik Jaringan untuk Deteksi Serangan Flooding pada Web Server,” 2017.

[12] M. Clearos, “Implementasi keamanan instrusion detection system (ids) dan instrusion prevention system (ips) menggunakan clearos”.

[13] S. Dwivedi, M. Vardhan, S. Tripathi, and A. Kumar, “Implementation of adaptive scheme in evolutionary technique for anomaly ‑ based intrusion detection,” *Evol. Intell.*, no. 0123456789, 2019, doi: 10.1007/s12065-019-00293-8.

[14] M. V Pawar and J. Anuradha, “Network Security and Types of Attacks in Network,” *Procedia - Procedia Comput. Sci.*, vol. 48, no. Iccc, pp. 503–506, 2017, doi: 10.1016/j.procs.2015.04.126.

[15] Y. A. Utomo *et al.*, “MEMBANGUN SISTEM ANALISIS MALWARE PADA APLIKASI ANDROID DENGAN METODE REVERSE ENGINEERING MENGGUNAKAN REMNUX,” vol. 4, no. 3, pp. 2000–2012, 2018.

[16] A. C. Cinar and T. B. Kara, “The current state and future of mobile security in the light of the recent mobile security threat reports The current state and future of mobile security,” no. January, 2023, doi: 10.1007/s11042-023-14400-6.

[17] A. Heryandi and S. Atin, “Blockchain-based Trust , Transparent , Traceable Modeling on Learning Recognition System Kampus Merdeka,” vol. 22, no. 2, pp. 339–352, 2023, doi: 10.30812/matrik.v22i2.2780.

[18] K. Alfalqi, R. Alghamdi, and M. Waqdan, “Android Platform Malware Analysis,” vol. 6, no. 1, pp. 140–146, 2015.

[19] F. E. Nastiti and D. Hariyadi, “TELEGRAMBOT : USING TELEGRAM TO CRAWLING MALWARE,” vol. 4, no. 1, pp. 51–55, 2019.

[20] B. I. Darmawan and F. Yudha, “SIMULASI DAN ANALISIS ENCRYPTION BASED”.

[21] K. A. Safitri and U. K. Indonesia, “Strategi Keamanan Sistem Informasi untuk Melawan Serangan Ransomware,” no. April, 2023.

[22] M. Gheisari and G. Wang, “A Survey on Deep Learning in Big Data,” 2017, doi: 10.1109/CSE-EUC.2017.215.

[23] L. Zhang and L. Corporation, “Deep Learning for Sentiment Analysis : A Survey”.

[24] F. Kirom, “Studi Literatur : Macam-Macam Metode Mengunakan Pendekatan Deep Learning dan Contoh Penerapanya,” pp. 20–22, 2018.

[25] F. P. Rachman and H. Santoso, “Perbandingan Model Deep Learning untuk Klasifikasi Sentiment Analysis dengan Teknik Natural Languange Processing,” *J. Teknol. dan Manaj. Inform.*, vol. 7, no. 2, pp. 103–112, 2021.

[26] X. Wang and I. J. E. Beck, “Deep Learning,” 2018.

[27] A. L. Maas and A. Y. Ng, “Rectifier Nonlinearities Improve Neural Network Acoustic Models,” vol. 28, 2019.

[28] G. E. Hinton, “Rectified Linear Units Improve Restricted Boltzmann Machines,” no. 3.

[29] J. Universitas *et al.*, “Mal-Detect : Pendekatan visualisasi cerdas untuk mendeteksi malware Machine Translated by Google,” vol. 34, pp. 1968–1983, 2022.

[30] M. I. Abas and U. M. Gorontalo, “PREDIKSI RENTET WAKTU JUMLAH PENUMPANG BANDARA MENGGUNAKAN ALGORITMA NEURAL NETWORK BERBASIS GENETIC ALGORITHM,” no. January 2020, 2021.

[31]. V. Nair and G. E. Hinton, "Rectified linear units improve restricted boltzmann machines," in Proceedings of the 27th International Conference on Machine Learning (ICML-10), 2010, pp. 807-814.

[32]. J. T. Townsend, "Theoretical analysis of an alphabetic confusion matrix," Perception & Psychophysics, vol. 9, pp. 40-50, 1971.

[33]. R. Maesarah, "Metode Deteksi Malware Menggunakan Support Vector Machine (SVM) dan Artificial Neural Network (ANN)," PhD Thesis, Universitas Gadjah Mada, 2023.

[34]. T. Bourlai, "Automatic Detection of Android Malware using Deep Neural Networks," in Proceedings of the International Conference on Cyber

Security, 2021.

[35]. D. W. A. Asry, E. Siswanto, D. Kurniawan, dan H. I. Huda, "Deteksi Malware Statis Pada Portable Executable Menggunakan Deep Neural Network," Jurnal Nama Jurnal, vol. 10, no. 2, pp. 123-135, 2021.

[36]. A. Ashrafa, A. Aziza, U. Zahooraa, M. Rajarajan, and A. Khan, "Analisis Ransomware Feature Engineering dan Deep Neural Networks," Jurnal Nama Jurnal, vol. 10, no. 2, pp. 45-60, 2022.

[37]. V. K. and M. S. V., "Deteksi Malware: Gist Features dan Deep Neural Network," Gist, vol. 9, no. 2, pp. 123-145, 2020.

[38]. P. Sreekumari, "Teknik Deteksi Malware menggunakan Deep Learning," Journal of Cybersecurity, vol. 3, no. 2, pp. 45-58, 2020.

[39]. A. Prayoga, et al., "Arsitektur Convolutional Neural Network untuk Model Klasifikasi Citra Batik Yogyakarta," Journal of Applied Computer Science and Technology, vol. 4, no. 2, pp. 82-89, 2023.