DAFTAR PUSTAKA

[1] Z. Arifin and M. Kom, “Keamanan dan Ancaman pada Cyberspace”.

[2] “Definisi Keamanan Informasi & 3 Aspek Di dalamnya | Agus Hermanto.” Accessed: Jul. 27, 2024. [Online]. Available: https://www.agus-hermanto.com/blog/detail/definisi-keamanan-informasi-3-aspek-di-dalamnya

[3] A. Ramdan, N. Widyasono, and H. Mubarok, “Prediksi Jaringan TOR dan VPN menggunakan Algoritma K-Nearest Neighbour pada Trafik Darknet,” *Jurnal Sistem Cerdas*, pp. 21–35, 2022.

[4] “Apa itu Malware? Definisi, Jenis, dan Perlindungan Malware.” Accessed: Jul. 27, 2024. [Online]. Available: https://www.malwarebytes.com/malware

[5] F. A. Aboaoja, A. Zainal, F. A. Ghaleb, B. A. S. Al-rimy, T. A. E. Eisa, and A. A. H. Elnour, “Malware Detection Issues, Challenges, and Future Directions: A Survey,” 2022. doi: 10.3390/app12178482.

[6] M. Dener, G. Ok, and A. Orman, “Malware Detection Using Memory Analysis Data in Big Data Environment,” *Applied Sciences (Switzerland)*, vol. 12, no. 17, 2022, doi: 10.3390/app12178604.

[7] R.- Budiarto and Y. D. Kuntjoro, “Analisis Perilaku Entitas untuk Pendeteksian Serangan Internal Menggunakan Kombinasi Model Prediksi Memori dan Metode PCA,” *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 6, 2023, doi: 10.25126/jtiik.1067123.

[8] J. Kim, Y. Ban, E. Ko, H. Cho, and J. H. Yi, “MAPAS: a practical deep learning-based android malware detection system,” *Int J Inf Secur*, vol. 21, no. 4, 2022, doi: 10.1007/s10207-022-00579-6.

[9] S. Ogawa and H. Mori, “Application of evolutionary deep neural netwok to photovoltaic generation forecasting,” in *Proceedings - IEEE International Symposium on Circuits and Systems*, 2019. doi: 10.1109/ISCAS.2019.8702210.

[10] X. Xing, X. Jin, H. Elahi, H. Jiang, and G. Wang, “A Malware Detection Approach Using Autoencoder in Deep Learning,” *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3155695.

[11] M. M. Alani and A. I. Awad, “AdStop: Efficient flow-based mobile adware detection using machine learning,” *Comput Secur*, vol. 117, 2022, doi: 10.1016/j.cose.2022.102718.

[12] J. Park and S. Jung, “Android Adware Detection using Soot and CFG,” *J Wirel Mob Netw Ubiquitous Comput Dependable Appl*, vol. 13, no. 4, 2022, doi: 10.58346/JOWUA.2022.I4.006.

[13] S. Suresh, F. Di Troia, K. Potika, and M. Stamp, “An analysis of Android adware,” *Journal of Computer Virology and Hacking Techniques*, vol. 15, no. 3, 2019, doi: 10.1007/s11416-018-0328-8.

[14] F. Hussain *et al.*, “A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks,” *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3131014.

[15] M. A. Haq, “DBoTPM: A Deep Neural Network-Based Botnet Prediction Model,” *Electronics (Switzerland)*, vol. 12, no. 5, 2023, doi: 10.3390/electronics12051159.

[16] A. Arshad *et al.*, “A novel ensemble method for enhancing Internet of Things device security against botnet attacks,” *Decision Analytics Journal*, vol. 8, 2023, doi: 10.1016/j.dajour.2023.100307.

[17] N. M. S. Surameery and M. Y. Shakor, “Use Chat GPT to Solve Programming Bugs,” *International Journal of Information technology and Computer Engineering*, no. 31, 2023, doi: 10.55529/ijitc.31.17.22.

[18] T. Hirsch and B. Hofer, “Using textual bug reports to predict the fault category of software bugs,” *Array*, vol. 15, 2022, doi: 10.1016/j.array.2022.100189.

[19] G. Rodríguez-Pérez, G. Robles, A. Serebrenik, A. Zaidman, D. M. Germán, and J. M. Gonzalez-Barahona, “How bugs are born: a model to identify how bugs are introduced in software components,” *Empir Softw Eng*, vol. 25, no. 2, 2020, doi: 10.1007/s10664-019-09781-y.

[20] M. Manoj and V. G. Rani, “Ransomeware classification using fuzzy neural network algorithm,” *Int J Health Sci (Qassim)*, 2022, doi: 10.53730/ijhs.v6ns2.8026.

[21] S. Sharma and S. Singh, “Texture-Based Automated Classification of Ransomware,” *Journal of The Institution of Engineers (India): Series B*, vol. 102, no. 1, 2021, doi: 10.1007/s40031-020-00499-w.

[22] Aruna, Vivekanadan S J, Reni Hena Helan R, and Abirami G, “Comparative Analysis of Ransomeware Using Deep Learning,” *International Journal of Advanced Research in Science, Communication and Technology*, 2022, doi: 10.48175/ijarsct-4813.

[23] D. P. Pham, D. Marion, and A. Heuser, “ULTRA: Ultimate Rootkit Detection over the Air,” in *ACM International Conference Proceeding Series*, 2022. doi: 10.1145/3545948.3545962.

[24] S. Suresh Kumar and T. SudalaiMuthu, “Kernel Rootkit Secret Detection in Cloud Computing,” in *2022 1st International Conference on Computational Science and Technology, ICCST 2022 - Proceedings*, 2022. doi: 10.1109/ICCST55948.2022.10040354.

[25] Ronal Hadi, Y. Yuliana, and H. A. Mooduto, “Deteksi Ancaman Keamanan Pada Server dan Jaringan Menggunakan OSSEC,” *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 3, no. 1, 2022, doi: 10.30630/jitsi.3.1.58.

[26] M. K. Qabalin, M. Naser, and M. Alkasassbeh, “Android Spyware Detection Using Machine Learning: A Novel Dataset,” *Sensors*, vol. 22, no. 15, 2022, doi: 10.3390/s22155765.

[27] J. R. Cares, “SPYWARE,” in *Encyclopedia of Cyber Warfare*, 2017. doi: 10.22214/ijraset.2022.42200.

[28] C. Guo, D. Luo, G. W. Shen, Y. H. Cui, and Y. Ping, “A Spyware Detection Method based on Inducement Mechanism,” *Tien Tzu Hsueh Pao/Acta Electronica Sinica*, vol. 50, no. 4, 2022, doi: 10.12263/DZXB.20211017.

[29] M. Mutalazimah and L. Mustikaningrum, “Knowledge about intestinal worm infection and helminthiasis in pregnant women,” *Electronic Journal of General Medicine*, vol. 17, no. 3, 2020, doi: 10.29333/ejgm/7876.

[30] J. Li, D. Sisodia, and S. Stafford, “On the Detection of Smart, Self-Propagating Internet Worms,” *IEEE Trans Dependable Secure Comput*, vol. 20, no. 4, 2023, doi: 10.1109/TDSC.2022.3194127.

[31] A. E. Chakroun *et al.*, “Numerical and experimental study of the dynamic behaviour of a polymer-metal worm drive,” *Mech Syst Signal Process*, vol. 193, 2023, doi: 10.1016/j.ymssp.2023.110263.

[32] S. Sutarti and E. Saepudin, “IMPLEMENTASI BITDEFENDER CORPORATE SECURITY UNTUK TROUBLESHOOTING PADA METROPOLITAN AREA NETWORK,” *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, vol. 9, no. 2, 2022, doi: 10.30656/prosisko.v9i2.5370.

[33] F. Syaifunazhirin, N. A. Saputra, A. Nihayah, I. Utmurtia, and D. F. Saputra, “Penerapan sistem keamanan jaringan pada kursus komputer menggunakan mikrotik,” *INTEGRATED (Journal of Information Technology and Vocational Education)*, vol. 4, no. 2, 2022, doi: 10.17509/integrated.v4i2.51524.

[34] A. Fausto, G. Gaggero, F. Patrone, and M. Marchese, “Reduction of the Delays Within an Intrusion Detection System (IDS) Based on Software Defined Networking (SDN),” *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3214974.

[35] P. Vanin *et al.*, “A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning,” 2022. doi: 10.3390/app122211752.

[36] Z. S. Zubi and A. W. M. Ibrahim, “Use of Naive Bayesian Filtering in the Intrusion Detection System (IDS),” *International Journal of Circuits, Systems and Signal Processing*, vol. 16, 2022, doi: 10.46300/9106.2022.16.102.

[37] B. Wijaya and A. Pratama, “Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort,” vol. 09, pp. 97–101, 2020.

[38] W. Muftihaturrahmah, T. Sau, and S. Siswantyo, “Analisis Penggunaan Hasil Deteksi IDS Snort pada Tools RITA dalam Mendeteksi Aktivitas Beacon,” no. 1.

[39] I. Muhamad Malik Matin, “Hyperparameter Tuning Menggunakan GridsearchCV pada Random Forest untuk Deteksi Malware,” *MULTINETICS*, vol. 9, no. 1, 2023, doi: 10.32722/multinetics.v9i1.5578.

[40] A. A. PRAMUDITA, A. R. DWINANDA, B. S. NUGRAHA, and H. H. RYANU, “Metode Reduksi Clutter Dinamis pada Sistem Radar-Drone untuk Deteksi Tanda Vital Pernafasan,” *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, vol. 12, no. 1, 2024, doi: 10.26760/elkomika.v12i1.148.

[41] Dieta Wahyu Asry, Eko Siswanto, Dendy Kurniawan, and Haris Ihsanil Huda, “Deteksi Malware Statis Menggunakan Deep Neural Networks Pada Portable Executable,” *Teknik: Jurnal Ilmu Teknik dan Informatika*, vol. 3, no. 1, 2023, doi: 10.51903/teknik.v3i1.325.

[42] Muhammad Nur Faiz, Oman Somantri, and Arif Wirawan Muhammad, “Rekayasa Fitur Berbasis Machine Learning untuk Mendeteksi Serangan DDoS,” *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 11, no. 3, 2022, doi: 10.22146/jnteti.v11i3.3423.

[43] R. Nindyasari, “METODE NON- HEURISTIC UNTUK DETEKSI REFACTORING NON-SOURCE CODE (SYSTEMATIC LITERATURE REVIEW),” *Simetris : Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, vol. 6, no. 2, 2015, doi: 10.24176/simet.v6i2.473.

[44] S. A. Valianta, T. Salim, and D. Stiawan, “Identifikasi Serangan Port Scanning dengan Metode String Matching,” *Annual Research Seminar (ARS)*, vol. 2, no. Fakultas Ilmu Komputer Unsri, 2016.

[45] M. Yousef and J. Allmer, “Deep learning in bioinformatics,” *Turkish Journal of Biology*, vol. 47, no. 6, 2023, doi: 10.55730/1300-0152.2671.

[46] S. Shukla, N. Badal, and B. K. Thakur, “Introduction to Deep Learning,” in *Sustainable Computing: Transforming Industry 4.0 to Society 5.0*, 2023. doi: 10.1007/978-3-031-13577-4_15.

[47] R. A. de Oliveira and M. H. J. Bollen, “Deep learning for power quality,” 2023. doi: 10.1016/j.epsr.2022.108887.

[48] C. Huang, J. Wang, S. Wang, and Y. Zhang, “A review of deep learning in dentistry,” *Neurocomputing*, vol. 554, 2023, doi: 10.1016/j.neucom.2023.126629.

[49] M. M. Taye, “Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions,” 2023. doi: 10.3390/computers12050091.

[50] N. Shlezinger, J. Whang, Y. C. Eldar, and A. G. Dimakis, “Model-Based Deep Learning,” *Proceedings of the IEEE*, vol. 111, no. 5, 2023, doi: 10.1109/JPROC.2023.3247480.

[51] Z. Liu *et al.*, “Deep learning based brain tumor segmentation: a survey,” *Complex and Intelligent Systems*, vol. 9, no. 1, 2023, doi: 10.1007/s40747-022-00815-5.

[52] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, “Blockchain for deep learning: review and open challenges,” *Cluster Comput*, vol. 26, no. 1, 2023, doi: 10.1007/s10586-022-03582-7.

[53] A. Mohammed and R. Kora, “A comprehensive review on ensemble deep learning: Opportunities and challenges,” 2023. doi: 10.1016/j.jksuci.2023.01.014.

[54] E. Matel, F. Vahdatikhaki, S. Hosseinyalamdary, T. Evers, and H. Voordijk, “An artificial neural network approach for cost estimation of engineering services,” *International Journal of Construction Management*, vol. 22, no. 7, 2022, doi: 10.1080/15623599.2019.1692400.

[55] M. A. Obeidat, B. N. A. Ameryeen, A. M. Mansour, H. Al Salem, and A. M. E. Awwad, “Wind Power Forecasting using Artificial Neural Network,” *WSEAS Transactions on Power Systems*, vol. 17, 2022, doi: 10.37394/232016.2022.17.28.

[56] N. N. A. Mangshor, S. Ibrahim, N. Sabri, and S. A. Kamaruddin, "Students' learning habit factors during COVID-19 pandemic using multilayer perceptron (MLP)," *International Journal of Advanced Technology and Engineering Exploration*, vol. 8, no. 74, 2021, doi: 10.19101/IJATEE.2020.S1762140.

[57] T. Kattenborn, J. Leitloff, F. Schiefer, and S. Hinz, "Review on Convolutional Neural Networks (CNN) in vegetation remote sensing," 2021. doi: 10.1016/j.isprsjprs.2020.12.010.

[58] F. Shan, X. He, D. J. Armaghani, and D. Sheng, "Effects of data smoothing and recurrent neural network (RNN) algorithms for real-time forecasting of tunnel boring machine (TBM) performance," *Journal of Rock Mechanics and Geotechnical Engineering*, vol. 16, no. 5, 2024, doi: 10.1016/j.jrmge.2023.06.015.

[59] X. Ding, X. Hou, M. Xia, Y. Ismail, and J. Ye, "Predictions of macroscopic mechanical properties and microscopic cracks of unidirectional fibre-reinforced polymer composites using deep neural network (DNN)," *Compos Struct*, vol. 302, 2022, doi: 10.1016/j.compstruct.2022.116248.

[60] W. J. Song, S. G. Choi, and E. S. Lee, "Prediction and comparison of electrochemical machining on shape memory alloy(SMA) using deep neural network(DNN)," *Journal of Electrochemical Science and Technology*, vol. 10, no. 3, 2019, doi: 10.33961/jecst.2019.03174.

[61] A. Müller and A. Taras, "Prediction of the local buckling strength and load-displacement behaviour of SHS and RHS members using Deep Neural Networks (DNN) – Introduction to the Deep Neural Network Direct Stiffness Method (DNN-DSM)," *Steel Construction*, vol. 15, 2022, doi: 10.1002/stco.202100047.

[62] Z. Wan, Z. Chang, Y. Xu, and B. Šavija, "Optimization of vascular structure of self-healing concrete using deep neural network (DNN)," *Constr Build Mater*, vol. 364, 2023, doi: 10.1016/j.conbuildmat.2022.129955.

[63] N. D. Al-Shakarchy and I. H. Ali, "Detecting abnormal movement of driver's head based on spatial-temporal features of video using deep neural network DNN," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 1, 2020, doi: 10.11591/ijeecs.v19.i1.pp344-352.

[64] R. B. Hadiprakoso, N. Qomariasih, and R. N. Yasa, "Identifikasi Malware Android Menggunakan Pendekatan Analisis Hibrid Dengan Deep Learning," *Jurnal Teknologi Informasi Universitas Lambung Mangkurat (JTIULM)*, vol. 6, no. 2, pp. 77–84, 2021, doi: 10.20527/jtiulm.v6i2.82.

[65] E. C. Bayazit, O. K. Sahingoz, and B. Dogan, “Deep Learning based Malware Detection for Android Systems: A Comparative Analysis,” *Tehnicki Vjesnik*, vol. 30, no. 3, pp. 787–796, 2023, doi: 10.17559/TV-20220907113227.

[66] M. Tokmak, E. U. Küçüksille, and U. Köse, “Deep Learning Based Malware Detection Tool Development for Android Operating System,” *BRAIN. Broad Research in Artificial Intelligence and Neuroscience*, vol. 12, no. 4, pp. 28–56, 2021, doi: 10.18662/brain/12.4/237.

[67] T. Informatics and E. Vol, “ADVANCED MALICIOUS SOFTWARE DETECTION USING DNN Sulartopo 1 , Dani Sasmoko 2 , Zaenal Mustofa 3 , Arsito Ari Kuncoro 4 Universita Sains dan Teknologi Komputer,” vol. 1, no. 1, pp. 80–107, 2022.

[68] O. N. Elayan and A. M. Mustafa, “Android malware detection using deep learning,” *Procedia Computer Science*, vol. 184, no. 2019, pp. 847–852, 2021, doi: 10.1016/j.procs.2021.03.106.

[69] Didih Rizki Chandranegara, Jafar Shodiq Djawas, Faiq Azmi Nurfaizi, and Zamah Sari, “Malware Image Classification Using Deep Learning InceptionResNet-V2 and VGG-16 Method,” *Jurnal Online Informatika*, vol. 8, no. 1, pp. 61–71, 2023, doi: 10.15575/join.v8i1.1051.

[70] S. Lu, Q. Li, and X. Zhu, “Stealthy Malware Detection Based on Deep Neural Network,” *Journal of Physics: Conference Series*, vol. 1437, no. 1, 2020, doi: 10.1088/1742-6596/1437/1/012123.

[71] Didih Rizki Chandranegara, Jafar Shodiq Djawas, Faiq Azmi Nurfaizi, and Zamah Sari, “Malware Image Classification Using Deep Learning InceptionResNet-V2 and VGG-16 Method,” *Jurnal Online Informatika*, vol. 8, no. 1, pp. 61–71, 2023, doi: 10.15575/join.v8i1.1051.

[72] N. Afifah and D. Stiawan, “The Implementation of Deep Neural Networks Algorithm for Malware Classification,” *Computer Engineering and Applications Journal*, vol. 8, no. 3, pp. 189–202, 2019, doi: 10.18495/comengapp.v8i3.294.

[73] “Malware Memory Analysis | Datasets | Canadian Institute for Cybersecurity | UNB.” Accessed: Jul. 27, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/malmem-2022.html

[74] S. S. Shafin, G. Karmakar, and I. Mareels, “Obfuscated Memory Malware Detection in Resource-Constrained IoT Devices for Smart City Applications,” *Sensors*, vol. 23, no. 11, pp. 1–18, 2023, doi: 10.3390/s23115348.

[75] E. A. Winanto, K. Kurniabudi, S. Sharipuddin, I. S. Wijaya, and D. Sandra, "Deteksi Serangan pada Jaringan Kompleks IoT menggunakan Recurrent Neural Network," *JURIKOM (Jurnal Riset Komputer)*, vol. 9, no. 6, p. 1996, 2022, doi: 10.30865/jurikom.v9i6.5298.

[76] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Bin Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection," *IEEE Access*, vol. 8, pp. 132911–132921, 2020, doi: 10.1109/ACCESS.2020.3009843.

[77] K. Kurniabudi, A. Harris, and A. Rahim, "Seleksi Fitur Dengan Information Gain Untuk Meningkatkan Deteksi Serangan DDoS menggunakan Random Forest," *Techno.Com*, vol. 19, no. 1, pp. 56–66, 2020, doi: 10.33633/tc.v19i1.2860.

[78] E. V. Tjahjadi and B. Santoso, "Klasifikasi Malware Menggunakan Teknik Machine Learning," *Jurnal Ilmiah Ilmu Komputer*, vol. 2, no. 1, pp. 60–70, 2023.

[79] R. Galih, "Deteksi Malware Android Menggunakan Pengklasifikasi Pembelajaran Mesin Paralel," vol. 10, no. 5, pp. 4887–4895, 2023.

[80] R. Galih, "Deteksi Malware Android Menggunakan Pengklasifikasi Pembelajaran Mesin Paralel," vol. 10, no. 5, pp. 4887–4895, 2023.

[81] T. Carrier, P. Victor, A. Tekeoglu, and A. Lashkari, "Detecting Obfuscated Malware using Memory Feature Engineering," no. Icissp, pp. 177–188, 2022, doi: 10.5220/0010908200003120.

[82] I. Muhamad Malik Matin, "Hyperparameter Tuning Menggunakan GridsearchCV pada Random Forest untuk Deteksi Malware," *Multinetics*, vol. 9, no. 1, pp. 43–50, 2023, doi: 10.32722/multinetics.v9i1.5578.

[83] Togu Novriansyah Turnip, Chatrine Febryanti Manurung, Yogi Septian Lubis, and Rachel Gultom, "Klasifikasi Malware Android Aplikasi Menggunakan Random Forest Berdasarkan Fitur Statik," *Teknik Informatika dan Sistem Informasi*, vol. 10, no. 1, pp. 926–936, 2023.

[84] K. Y. Chan *et al.*, "Deep neural networks in the cloud: Review, applications, challenges and research directions," *Neurocomputing*, vol. 545, p. 126327, 2023, doi: 10.1016/j.neucom.2023.126327.

[85] M. Hibat-Allah, M. Ganahl, L. E. Hayward, R. G. Melko, and J. Carrasquilla, "Recurrent neural network wave functions," *Physical Review Research*, vol. 2, no. 2, pp. 1–17, 2020, doi: 10.1103/PhysRevResearch.2.023358.

[86] Baiq Nurul Azmi, Arief Hermawan, and Donny Avianto, "Analisis Pengaruh Komposisi Data Training dan Data Testing pada Penggunaan PCA dan

Algoritma Decision Tree untuk Klasifikasi Penderita Penyakit Liver," *JTIM : Jurnal Teknologi Informasi dan Multimedia*, vol. 4, no. 4, pp. 281–290, 2023, doi: 10.35746/jtim.v4i4.298.

[87] A. Nurhopipah and U. Hasanah, "Dataset Splitting Techniques Comparison For Face Classification on CCTV Images," *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, vol. 14, no. 4, p. 341, 2020, doi: 10.22146/ijccs.58092.

[88] D. S. Suparno, "Pengenalan Pola Untuk Mengetahui Jumlah Target Pengunjung Mall Berdasarkan Usia, Gender, Pendapatan Pertahun, Pengeluaran, Tujuannya Untuk Mempermudah Mengetahui Target Pasar Menggunakan Metode EDA, K-Means, Hierarchial Clustering, Confusion Matrix," *Sains, Aplikasi, Komputasi, dan Teknologi Informasi*, vol. 3, no. 2, pp. 61–69, 2021.

[89] Dieta Wahyu Asry, Eko Siswanto, Dendy Kurniawan, and Haris Ihsanil Huda, "Deteksi Malware Statis Menggunakan Deep Neural Networks Pada Portable Executable," *Teknik: Jurnal Ilmu Teknik dan Informatika*, vol. 3, no. 1, pp. 19–34, 2023, doi: 10.51903/teknik.v3i1.325.

[90] F. Bourebaa and M. Benmohamed, "A Deep Neural Network Model for Android Malware Detection," *International Journal of Informatics and Applied Mathematics*, vol. 4, no. 1, pp. 1–14, 2020.

[91] N. Afifah and D. Stiawan, "The Implementation of Deep Neural Networks Algorithm for Malware Classification," *Computer Engineering and Applications Journal*, vol. 8, no. 3, pp. 189–202, 2019, doi: 10.18495/comengapp.v8i3.294.