DAFTAR PUSTAKA

[1] K. Phillips, J. C. Davidson, R. R. Farr, C. Burkhardt, S. Caneppele, and M. P. Aiken, "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies," Jun. 01, 2022, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/forensicsci2020028.

[2] Z. Pan, J. Sheldon, and P. Mishra, "Hardware-Assisted Malware Detection and Localization Using Explainable Machine Learning," *IEEE Transactions on Computers*, vol. 71, no. 12, pp. 3308–3321, Dec. 2022, doi: 10.1109/TC.2022.3150573.

[3] A. Petrosyan, "State of malware worldwide - Statistics & Facts," Statista. Accessed: Jun. 17, 2025. [Online]. Available: https://www.statista.com/topics/8338/malware/#topicOverview

[4] S. Duman, M. Buchler, M. Egele, and E. Kirda, "PellucidAttachment: Protecting Users From Attacks via E-Mail Attachments," *IEEE Trans Dependable Secure Comput*, vol. 21, no. 3, pp. 1342–1354, May 2024, doi: 10.1109/TDSC.2023.3279032.

[5] A. Iqbal, M. N. Aman, R. Rejendran, and B. Sikdar, "Unveiling the Connection Between Malware and Pirated Software in Southeast Asian Countries: A Case Study," *IEEE Open Journal of the Computer Society*, vol. 5, pp. 62–72, 2024, doi: 10.1109/OJCS.2024.3364576.

[6] Wasilaturrahmi, "Perancangan Sistem Analisis Dinamis dan Klasifikasi Malware Otomatis dengan Algoritma K-Nearest Neighbors," Bandung, 2021.

[7] M. R. Alfarisy, "Perancangan Sistem Analisa Dinamis dan Klasifikasi Malware Otomatis dengan Algoritma Random Forest," Bandung, 2020.

[8] R. H. Hidayat, "Perancangan Sistem Analisa Dinamis dan Klasifikasi Malware Otomatis dengan Metode Decision Tree," Bandung, 2021.

[9] Y. W, Y. B. Fitriana, S. Esabela, and F. Hamdani, "Deteksi Serangan Malware Pada Web Aplikasi Menggunakan Metode Malware Analis Dinamis dan Statis,"

Digital Transformation Technology, vol. 4, no. 1, pp. 461–470, Jul. 2024, doi: 10.47709/digitech.v4i1.4270.

[10] C. Gan, Q. Feng, X. Zhang, Z. Zhang, and Q. Zhu, "Dynamical Propagation Model of Malware for Cloud Computing Security," *IEEE Access*, vol. 8, pp. 20325–20333, Jan. 2020, doi: 10.1109/ACCESS.2020.2968916.

[11] J. Chandy, "Review on Malware, Types, and its Analysis," *Int J Res Appl Sci Eng Technol*, vol. 10, no. 12, pp. 386–390, Dec. 2022, doi: 10.22214/ijraset.2022.47887.

[12] Z. Juhasz, "Quantitative cost comparison of on-premise and cloud infrastructure based EEG data processing," *Cluster Comput*, vol. 24, no. 2, pp. 625–641, Jun. 2021, doi: 10.1007/s10586-020-03141-y.

[13] D. Golec, I. Strugar, and D. Belak, "The Benefits of Enterprise Data Warehouse Implementation in Cloud vs. On-premises," *ENTRENOVA - ENTerprise REsearch InNOVAtion*, vol. 7, no. 1, pp. 67–76, Dec. 2021, doi: 10.54820/dmzs9230.

[14] A. Wijoyo, D. Daffa Raihan, and M. Farhan Maulana, "Perbandingan Antara Sistem Informasi Manajemen Berbasis Cloud Computing dan ON-Premises: Keuntungan Dan Tantangan," *TEKNOBIS: Teknologi, Bisnis Dan Pendidikan*, vol. 1, no. 6, pp. 416–420, Apr. 2024, [Online]. Available: https://jurnalmahasiswa.com/index.php/teknobis

[15] A. Küchler, A. Mantovani, Y. Han, L. Bilge, and D. Balzarotti, "Does Every Second Count? Time-based Evolution of Malware Behavior in Sandboxes," 2021, doi: 10.14722/ndss.2021.24475ï.

[16] X. Ying, "An Overview of Overfitting and its Solutions," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Mar. 2019. doi: 10.1088/1742-6596/1168/2/022022.

[17] B. Baek, S. Euh, D. Baek, D. Kim, and D. Hwang, "Histogram Entropy Representation and Prototype Based Machine Learning Approach for Malware Family Classification," *IEEE Access*, vol. 9, pp. 152098–152114, 2021, doi: 10.1109/ACCESS.2021.3127195.

[18] J.-H. Hwang, J. Kwak, and T.-J. Lee, “Fast k-NN based Malware Analysis in a Massive Malware Environment,” *KSII Transactions on Internet and Information Systems*, vol. 13, no. 12, pp. 6145–6158, 2019, doi: 10.3837/tiis.2019.12.019.

[19] I. H. Sarker, “Machine Learning: Algorithms, Real-World Applications and Research Directions,” May 01, 2021, *Springer*. doi: 10.1007/s42979-021-00592-x.

[20] X. Ying, “An Overview of Overfitting and its Solutions,” in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Mar. 2019. doi: 10.1088/1742-6596/1168/2/022022.

[21] W. E. Mouhtadi, M. E. Bakkali, Y. Maleh, S. Mounir, and K. Ouazzane, “Refining Malware Detection With Enhanced Machine Learning Algorithms Using Hyperparameter Tuning,” *International Journal of Critical Computer-Based Systems*, vol. 11, no. 1–2, pp. 48–67, 2024, doi: 10.1504/IJCCBS.2024.139100.

[22] B. Hariharan, R. Siva, S. Sadagopan, V. Mishra, and Y. Raghav, “Malware Detection Using XGBoost based Machine Learning Models - Review,” in *Proceedings of the 2nd International Conference on Edge Computing and Applications, ICECAA 2023*, 2023, pp. 964–970. doi: 10.1109/ICECAA58104.2023.10212327.

[23] Z. Akhtar, “Malware Detection and Analysis: Challenges and Research Opportunities,” Jan. 2021, [Online]. Available: http://arxiv.org/abs/2101.08429

[24] O. Aslan and R. Samet, “A Comprehensive Review on Malware Detection Approaches,” 2020, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2019.2963724.

[25] O. Aslan, M. Ozkan-Okay, and D. Gupta, “Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment,” *IEEE Access*, vol. 9, pp. 83252–83271, 2021, doi: 10.1109/ACCESS.2021.3087316.

[26] A. Fedák and J. Štulrajter, “Fundametals of Static Malware Analysis: Principles, Methods and Tools,” 2020. [Online]. Available: www.virscan.org

[27] R. Baker del Aguila, C. D. Contreras Pérez, A. G. Silva-Trujillo, J. C. Cuevas-Tello, and J. Nunez-Varela, “Static Malware Analysis Using Low-Parameter

Machine Learning Models," *Computers*, vol. 13, no. 3, Mar. 2024, doi: 10.3390/computers13030059.

[28] E. Debas, N. Alhumam, and K. Riad, "Unveiling the Dynamic Landscape of Malware Sandboxing: A Comprehensive Review," Dec. 14, 2023. doi: 10.20944/preprints202312.1009.v1.

[29] M. S. Akhtar and T. Feng, "Malware Analysis and Detection Using Machine Learning Algorithms," *Symmetry (Basel)*, vol. 14, no. 11, Nov. 2022, doi: 10.3390/sym14112304.

[30] T. A. Assegie, "An Optimized KNN Model for Signature-Based Malware Detection," 2021, doi: 10.22362/ijcert/2021/v8/i2/v8i206.

[31] Q. Abu Al-Haija, A. Odeh, and H. Qattous, "PDF Malware Detection Based on Optimizable Decision Trees," *Electronics (Switzerland)*, vol. 11, no. 19, Oct. 2022, doi: 10.3390/electronics11193142.

[32] Y. Wu and Y. Chang, "Ransomware Detection on Linux Using Machine Learning with Random Forest Algorithm," Jun. 07, 2024. doi: 10.36227/techrxiv.171778770.06550236/v1.

[33] M. Wadkar, F. Di Troia, and M. Stamp, "Detecting malware evolution using support vector machines," *Expert Syst Appl*, vol. 143, Apr. 2020, doi: 10.1016/j.eswa.2019.113022.

[34] A. A. Taha and S. J. Malebary, "Hybrid classification of Android malware based on fuzzy clustering and the gradient boosting machine," *Neural Comput Appl*, vol. 33, no. 12, pp. 6721–6732, Jun. 2021, doi: 10.1007/s00521-020-05450-0.

[35] M. Yong Wong, M. Landen, M. Antonakakis, D. M. Blough, E. M. Redmiles, and M. Ahamad, "An Inside Look into the Practice of Malware Analysis," in *Proceedings of the ACM Conference on Computer and Communications Security*, Association for Computing Machinery, Nov. 2021, pp. 3053–3069. doi: 10.1145/3460120.3484759.

[36] S. Talukder and Z. Talukder, "A Survey on Malware Detection and Analysis Tools," *International Journal of Network Security & Its Applications*, vol. 12, no. 2, pp. 37–57, Mar. 2020, doi: 10.5121/ijnsa.2020.12203.

[37] M. S. Karvandi *et al.*, “HyperDbg: Reinventing Hardware-Assisted Debugging,” in *Proceedings of the ACM Conference on Computer and Communications Security*, Association for Computing Machinery, Nov. 2022, pp. 1709–1723. doi: 10.1145/3548606.3560649.

[38] B. Rashmitha, J. Alwina, B. Angelin, and E. R. Ramesh, “Malware analysis and detection using reverse Engineering.” [Online]. Available: https://github.com/glmcdona/strings2.

[39] B. Rashmitha, J. Alwina, B. Angelin, and E. R. Ramesh, “Malware analysis and detection using reverse Engineering.” [Online]. Available: https://github.com/glmcdona/strings2.

[40] Y. Birman, S. Hindi, G. Katz, and A. Shabtai, “Cost-Effective Malware Detection as a Service over Serverless Cloud Using Deep Reinforcement Learning,” in *Proceedings - 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing, CCGRID 2020*, Institute of Electrical and Electronics Engineers Inc., May 2020, pp. 420–429. doi: 10.1109/CCGrid49817.2020.00-51.

[41] A. Patel and R. Kumar, “From On-Premise to Cloud: Evolving Cybersecurity Measures for Modern Enterprises.”

[42] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, “A bidirectional LSTM deep learning approach for intrusion detection,” *Expert Syst Appl*, vol. 185, Dec. 2021, doi: 10.1016/j.eswa.2021.115524.

[43] D. Naik and C. D. Jaidhar, “A novel Multi-Layer Attention Framework for visual description prediction using bidirectional LSTM,” *J Big Data*, vol. 9, no. 1, Dec. 2022, doi: 10.1186/s40537-022-00664-6.

[44] M. Ma, C. Liu, R. Wei, B. Liang, and J. Dai, “Predicting machine’s performance record using the stacked long short-term memory (LSTM) neural networks,” *J Appl Clin Med Phys*, vol. 23, no. 3, Mar. 2022, doi: 10.1002/acm2.13558.

[45] M. Ayitey Junior, P. Appiahene, and O. Appiah, “Forex market forecasting with two-layer stacked Long Short-Term Memory neural network (LSTM) and correlation analysis,” *Journal of Electrical Systems and Information Technology*, vol. 9, no. 1, Dec. 2022, doi: 10.1186/s43067-022-00054-1.

[46] Q. Kang, E. J. Chen, Z. C. Li, H. Bin Luo, and Y. Liu, “Attention-based LSTM predictive model for the attitude and position of shield machine in tunneling,” *Underground Space (China)*, vol. 13, pp. 335–350, Dec. 2023, doi: 10.1016/j.undsp.2023.05.006.

[47] Q. Kang, E. J. Chen, Z. C. Li, H. Bin Luo, and Y. Liu, “Attention-based LSTM predictive model for the attitude and position of shield machine in tunneling,” *Underground Space (China)*, vol. 13, pp. 335–350, Dec. 2023, doi: 10.1016/j.undsp.2023.05.006.

[48] Sebastián Ramírez, “FastAPI Documentation.” Accessed: Dec. 29, 2024. [Online]. Available: https://fastapi.tiangolo.com/

[49] ReportLab Developers, “ReportLab User Guide.”

[50] CourtBouillon Developers, “WeasyPrint Documentation.”

[51] FPDF Contributors, “PyFPDF Documentation,” 2024, Accessed: Dec. 29, 2024. [Online]. Available: https://pyfpdf.readthedocs.io/en/latest/

[52] QEMU Developers, “QEMU Documentation.”

[53] P. Mell *et al.*, “Measuring the Common Vulnerability Scoring System base score equation,” Nov. 2022. doi: 10.6028/NIST.IR.8409.

[54] D. F. Priambodo, A. D. Rifansyah, and M. Hasbi, “Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating,” *Teknika*, vol. 12, no. 1, pp. 33–46, Feb. 2023, doi: 10.34148/teknika.v12i1.571.

[55] N. Sobahi and A. Bamabad, “Cyber-attacks Risk Analysis of a Connected Pulse Oximeter Device: A Threat Modeling Using STRIDE and DREAD Models,” *International Journal for Scientific Research*, vol. 3, no. 5, pp. 280–315, Mar. 2024, doi: 10.59992/ijsr.2024.v3n5p10.

[56] L. Yang, A. Ciptadi, I. Laziuk, A. Ahmadzadeh, and G. Wang, “BODMAS: An Open Dataset for Learning based Temporal Analysis of PE Malware,” in *4th Deep Learning and Security Workshop*, 2021.

[57] Python Developers, “PyQt5 - Comprehensive Python Bindings for Qt v5.” Accessed: Jul. 24, 2025. [Online]. Available: https://pypi.org/project/PyQt5/