REFERENCES

[1] O. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8. 2020. doi: 10.1109/ACCESS.2019.2963724.

[2] D. Gibert, C. Mateu, and J. Planes, "The rise of machine learning for detection and classification of malware: Research developments, trends and challenges," *Journal of Network and Computer Applications*, vol. 153. 2020. doi: 10.1016/j.jnca.2019.102526.

[3] Y. N. K. Y. N. Kunang and ..., "Analisis Forensik Malware Pada Platform Android.," *Anal. Forensik …*, 2022.

[4] J. Hemalatha, S. A. Roseline, S. Geetha, S. Kadry, and R. Damaševičius, "An efficient densenet-based deep learning model for Malware detection," *Entropy*, vol. 23, no. 3, 2021, doi: 10.3390/e23030344.

[5] S. A. Roseline, S. Geetha, S. Kadry, and Y. Nam, "Intelligent Vision-Based Malware Detection and Classification Using Deep Random Forest Paradigm," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3036491.

[6] and A. G. M. Aranitasi, A. Daci, "Mobile malware detection techniques using system calls," *Int. J. Eng. Res. Appl. www.ijera.com*, vol. 12, pp. 54–57, 2022.

[7] H. Alimardani and M. Nazeh, "A taxonomy on recent mobile malware: Features, analysis methods, and detection techniques," *ACM Int. Conf. Proceeding Ser.*, pp. 44–49, 2018, doi: 10.1145/3230467.3230478.

[8] D. Aprilliansyah, I. Riadi, and Sunardi, "Analysis of Remote Access Trojan Attack using Android Debug Bridge," *IJID (International J. Informatics Dev.*, vol. 10, no. 2, pp. 102–111, 2022, doi: 10.14421/ijid.2021.2839.

[9] X. Liu, X. Du, X. Zhang, Q. Zhu, H. Wang, and M. Guizani, "Adversarial samples on android malware detection systems for IoT systems," *Sensors (Switzerland)*, vol. 19, no. 4, 2019, doi: 10.3390/s19040974.

[10] H. Li, S. Zhou, W. Yuan, J. Li, and H. Leung, "Adversarial-Example Attacks Toward Android Malware Detection System," *IEEE Syst. J.*, vol. 14, no. 1, 2020, doi: 10.1109/JSYST.2019.2906120.

[11] P. S. Uttarwar, R. P. Tidke, D. S. Dandwate, and U. J. Tupe, "A Literature Review on Android-A Mobile Operating system," *Int. Res. J. Eng. Technol.*, no. September, 2021.

[12] A. Adekotujo, A. Odumabo, A. Adedokun, and O. Aiyeniko, "A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS," *Int. J. Comput. Appl.*, vol. 176, no. 39, 2020, doi: 10.5120/ijca2020920494.

[13] I. Castillo-Zúñiga, F. J. Luna-Rosas, L. C. Rodríguez-Martínez, J. Muñoz-Arteaga, J. I. López-Veyna, and M. A. Rodríguez-Díaz, "Internet data analysis methodology for cyberterrorism vocabulary detection, combining techniques of big data analytics, NLP and semantic web," *Int. J. Semant. Web Inf. Syst.*, vol. 16, no. 1, pp. 69–86, 2020, doi: 10.4018/IJSWIS.2020010104.

[14] A. E. Joseph, "Cybercrime definition," *Comput. Crime Res. Cent.*, no. June 2017, 2017.

[15] C. Donalds, C. Barclay, and K.-M. Osei-Bryson, "Towards a Cybercrime Classification Ontology," in *Cybercrime and Cybersecurity in the Global South*, 2022. doi: 10.1201/9781003028710-15.

[16] Techopedia, "What is Cybercrime? - Definition from Techopedia," *Techopedia*, 2018.

[17] M. A. Dennis, "cybercrime | Definition, Statistics, & Examples | Britannica," *Webpage*, 2019.

[18] I. Shhadat, B. Bataineh, A. Hayajneh, and Z. A. Al-Sharif, "The Use of Machine Learning Techniques to Advance the Detection and Classification of Unknown Malware," *Procedia Comput. Sci.*, vol. 170, pp. 917–922, 2020, doi: 10.1016/j.procs.2020.03.110.

[19] T. Eom, H. Kim, S. M. An, J. S. Park, and D. S. Kim, "Android malware detection using feature selections and random forest," *Proc. - 2018 4th Int. Conf. Softw. Secur. Assur. ICSSA 2018*, pp. 55–61, 2018, doi: 10.1109/ICSSA45270.2018.00023.

[20] T. Bhatia and R. Kaushal, "Malware detection in android based on dynamic analysis," *2017 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2017*, 2017, doi:

10.1109/CyberSecPODS.2017.8074847.

[21] A. Qamar, A. Karim, and V. Chang, “Mobile malware attacks: Review, taxonomy & future directions,” *Futur. Gener. Comput. Syst.*, vol. 97, pp. 887–909, 2019, doi: 10.1016/j.future.2019.03.007.

[22] B. Urooj, M. A. Shah, C. Maple, M. K. Abbasi, and S. Riasat, “Malware Detection: A Framework for Reverse Engineered Android Applications Through Machine Learning Algorithms,” *IEEE Access*, vol. 10, pp. 89031–89050, 2022, doi: 10.1109/ACCESS.2022.3149053.

[23] S. Shakya and M. Dave, “Analysis, Detection, and Classification of Android Malware using System Calls,” 2022.

[24] B. Rashmitha, J. Alwina, B. Angelin, and E. R. Ramesh, “Malware analysis and detection using reverse Engineering,” *Int. J. Comput. Sci. Inf. Technol. Res.*, vol. 10, no. 4.

[25] M. L. Anupama *et al.*, “Detection and robustness evaluation of android malware classifiers,” *J. Comput. Virol. Hacking Tech.*, vol. 18, no. 3, pp. 147–170, 2022, doi: 10.1007/s11416-021-00390-2.

[26] M. Sharma, “A Study on RAT (Remote Access Trojan),” *Acad. J. Forensic Sci.*, vol. 02, no. 02, 2019.

[27] T. P. Setia, A. P. Aldya, and N. Widiyasono, “Reverse Engineering untuk Analisis Malware Remote Access Trojan,” *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, 2019, doi: 10.26418/jp.v5i1.28214.

[28] “Strace - Trace System Calls and Signals,” 2021.

[29] Scikit-learn, “sklearn ensemble Random Forest Classifier,” *Scikit-Learn*, 2022.

[30] P. Banerjee, “Random Forest Classifier Tutorial | Kaggle,” 2019.

[31] Y. Pan, X. Ge, C. Fang, and Y. Fan, “A Systematic Literature Review of Android Malware Detection Using Static Analysis,” *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3002842.

[32] J. Qiu, J. Zhang, W. Luo, L. Pan, S. Nepal, and Y. Xiang, “A Survey of Android Malware Detection with Deep Neural Models,” *ACM Computing Surveys*, vol. 53, no. 6. 2021. doi: 10.1145/3417978.

[33] S. R. T. Mat, M. F. A. Razak, M. N. M. Kahar, J. M. Arif, and A. Firdaus, “A Bayesian probability model for Android malware detection,” *ICT Express*, vol. 8, no. 3, 2022, doi: 10.1016/j.icte.2021.09.003.

[34] T. Isohara, K. Takemori, and A. Kubota, “Kernel-based behavior analysis for android malware detection,” *Proc. - 2011 7th Int. Conf. Comput. Intell. Secur. CIS 2011*, pp. 1011–1015, 2011, doi: 10.1109/CIS.2011.226.

[35] Y. Zhou and X. Jiang, “Dissecting Android malware: Characterization and evolution,” *Proc. - IEEE Symp. Secur. Priv.*, pp. 95–109, 2012, doi: 10.1109/SP.2012.16.

[36] “2022 International Conference on Computer Communication and Informatics, ICCCI 2022,” *2018 Int. Conf. Comput. Commun. Informatics, ICCCI 2022*, 2018.

[37] M. Christodorescu and S. Jha, “Static analysis of executables to detect malicious patterns,” *Proc. 12th USENIX Secur. Symp.*, pp. 169–186, 2003.

[38] Y. Zhang, “Research into the engineering application of reverse engineering technology,” *J. Mater. Process. Technol.*, vol. 139, no. 1-3 SPEC, 2003, doi: 10.1016/S0924-0136(03)00513-2.

[39] S. W. Asher, S. Jan, G. Tsaramirsis, F. Q. Khan, A. Khalil, and M. Obaidullah, “Reverse engineering of mobile banking applications,” *Comput. Syst. Sci. Eng.*, vol. 38, no. 3, 2021, doi: 10.32604/CSSE.2021.016787.

[40] Z. Zhou, D. Chen, and S. (Shengquan) Xie, “Springer Series in Advanced Manufacturing,” *Thermoplast. Thermoplast. Compos.*, pp. 863–866, 2007.