

DAFTAR PUSTAKA

- [1] Lookout, “Mobile Threat Landscape Report: Q2 2024,” <https://www.lookout.com/threat-intelligence/report/q2-2024-mobile-landscape-threat-report>.
- [2] Zimperium, “2024 GLOBAL MOBILE THREAT REPORT,” 2024. Accessed: Nov. 28, 2024. [Online]. Available: https://go.crowdstrike.com/global-threat-report-2024.html?utm_campaign=cao&utm_content=crwd-cao-apj-sea-en-psp-x-wht-gtr-tct-x_x_x_x-x&utm_medium=sem&utm_source=goog&utm_term=global%20threat%20report&cq_cmp=10902423317&cq_plac=&gad_source=1&gclid=CjwKCAiAxqC6BhBcEiwAlXp45_HW_rGDpsOcQq8yxhjc4Et1MK8WQmKwaHL9TZMNuXF7Qta2YJc2jBoCthoQAvD_BwE
- [3] J. Lewis, “Economic Impact of Cybercrime — No Slowing Down,” Feb. 2018. Accessed: Nov. 28, 2024. [Online]. Available: <https://www.csis.org/analysis/economic-impact-cybercrime>
- [4] S. Millar, N. McLaughlin, J. Martinez del Rincon, and P. Miller, “Multi-view deep learning for zero-day Android malware detection,” *Journal of Information Security and Applications*, vol. 58, p. 102718, May 2021, doi: 10.1016/j.jisa.2020.102718.
- [5] I. Martín, J. A. Hernández, and S. de los Santos, “Machine-Learning based analysis and classification of Android malware signatures,” *Future Generation Computer Systems*, vol. 97, pp. 295–305, Aug. 2019, doi: 10.1016/j.future.2019.03.006.
- [6] C. Leka, C. Ntantogian, S. Karagiannis, E. Magkos, and V. S. Verykios, “A Comparative Analysis of VirusTotal and Desktop Antivirus Detection Capabilities,” in *2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA)*, IEEE, Jul. 2022, pp. 1–6. doi: 10.1109/IISA56318.2022.9904382.
- [7] A. Salem, S. Banescu, and A. Pretschner, “Maat: Automatically Analyzing VirusTotal for Accurate Labeling and Effective Malware Detection,” *ACM Transactions on Privacy and Security*, vol. 24, no. 4, pp. 1–35, Nov. 2021, doi: 10.1145/3465361.
- [8] A. Salem, “Towards Accurate Labeling of Android Apps for Reliable Malware Detection,” in *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, New York, NY, USA: ACM, Apr. 2021, pp. 269–280. doi: 10.1145/3422337.3447849.
- [9] L. A. Zadeh, “The role of fuzzy logic in the management of uncertainty in expert systems,” *Fuzzy Sets Syst*, vol. 11, no. 1–3, pp. 199–227, 1983, doi: 10.1016/S0165-0114(83)80081-5.
- [10] NIST, “Guide for conducting risk assessments,” Gaithersburg, MD, 2012. doi: 10.6028/NIST.SP.800-30r1.

- [11] C. Enyoghasi and F. Badurdeen, "SUSTAINABLE PRODUCT DESIGN DECISION-MAKING THROUGH INTEGRATED RISK LIKELIHOOD AND IMPACT ANALYSES," in *Proceedings of ASME 2023 18th International Manufacturing Science and Engineering Conference, MSEC 2023*, 2023. doi: 10.1115/msec2023-102037.
- [12] Z. Meskauskas and E. Kazanavicius, "About the New Methodology and XAI-Based Software Toolkit for Risk Assessment," *Sustainability (Switzerland)*, vol. 14, no. 9, 2022, doi: 10.3390/su14095496.
- [13] A. Salem, S. Banescu, and A. Pretschner, "Maat," *ACM Transactions on Privacy and Security*, vol. 24, no. 4, pp. 1–35, Nov. 2021, doi: 10.1145/3465361.
- [14] S. Zhu *et al.*, "Measuring and Modeling the Label Dynamics of Online Anti-Malware Engines," pp. 2361–2378, 2020.
- [15] A. Salem, "Towards Accurate Labeling of Android Apps for Reliable Malware Detection," in *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, New York, NY, USA: ACM, Apr. 2021, pp. 269–280. doi: 10.1145/3422337.3447849.
- [16] E. R. Harang and M. E. Rudd, "SOREL-20M: A Large Scale Benchmark Dataset for Malicious PE Detection," *ArXiv*, vol. abs/2012.07634, 2020.
- [17] Y. Ye, L. Wu, Z. Hong, and K. Huang, "A risk classification based approach for Android malware detection," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 2, pp. 959–981, 2017, doi: 10.3837/tiis.2017.02.018.
- [18] J. Mohamad Arif, M. F. Ab Razak, S. R. Tuan Mat, S. Awang, N. S. N. Ismail, and A. Firdaus, "Android mobile malware detection using fuzzy AHP," *Journal of Information Security and Applications*, vol. 61, 2021, doi: 10.1016/j.jisa.2021.102929.
- [19] M. Fleming and O. Olukoya, "A temporal analysis and evaluation of fuzzy hashing algorithms for Android malware analysis," *Forensic Science International: Digital Investigation*, vol. 49, 2024, doi: 10.1016/j.fsidi.2024.301770.
- [20] A. Altaher and O. Barukab, "Android malware classification based on ANFIS with fuzzy c-means clustering using significant application permissions," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 25, no. 3, pp. 2232–2242, 2017, doi: 10.3906/elk-1602-107.
- [21] A. Taha, O. Barukab, and S. Malebary, "Fuzzy integral-based multi-classifiers ensemble for android malware classification," *Mathematics*, vol. 9, no. 22, 2021, doi: 10.3390/math9222880.
- [22] M. Dhalaria and E. Gandotra, "Android Malware Risk Evaluation Using Fuzzy Logic," in *PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and Grid Computing*, 2022, pp. 341–345. doi: 10.1109/PDGC56933.2022.10053179.

- [23] D. Z. Syeda and M. N. Asghar, "Dynamic Malware Classification and API Categorisation of Windows Portable Executable Files Using Machine Learning," *Applied Sciences (Switzerland)*, vol. 14, no. 3, 2024, doi: 10.3390/app14031015.
- [24] M. Y. Muzayan Haq, A. Abhishta, S. Zeijlemaker, A. Chau, M. Siegel, and L. J. M. Nieuwenhuis, "Measuring Malware Detection Capability for Security Decision Making," in *Proceedings - 9th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2024*, 2024, pp. 342–351. doi: 10.1109/EuroSPW61312.2024.00044.
- [25] N. ‘. Sabri, S. Khamis, and Z. Zainudin, *Android Malware Detection Using Machine Learning Technique*, vol. 211. 2024. doi: 10.1007/978-3-031-59707-7_14.
- [26] A. Saracino, D. Sgandurra, G. Dini, and F. Martinelli, "MADAM: Effective and Efficient Behavior-based Android Malware Detection and Prevention," *IEEE Trans Dependable Secure Comput*, vol. 15, no. 1, pp. 83–97, Jan. 2018, doi: 10.1109/TDSC.2016.2536605.
- [27] Y. Pan, X. Ge, C. Fang, and Y. Fan, "A Systematic Literature Review of Android Malware Detection Using Static Analysis," *IEEE Access*, vol. 8, pp. 116363–116379, 2020, doi: 10.1109/ACCESS.2020.3002842.
- [28] A. Yewale and M. Singh, "Malware detection based on opcode frequency," in *Proceedings of 2016 International Conference on Advanced Communication Control and Computing Technologies, ICACCCT 2016*, 2017, pp. 646–649. doi: 10.1109/ICACCCT.2016.7831719.
- [29] F. T. Ngo, A. Agarwal, R. Govindu, and C. MacDonald, *Malicious software threats*. 2020. doi: 10.1007/978-3-319-78440-3_35.
- [30] Q. K. A. Mirza, M. Brown, O. Halling, L. Shand, and A. Alam, "Ransomware Analysis using Cyber Kill Chain," in *Proceedings - 2021 International Conference on Future Internet of Things and Cloud, FiCloud 2021*, 2021, pp. 58–65. doi: 10.1109/FiCloud49777.2021.00016.
- [31] H. Huseynov, K. Kourai, T. Saadawi, and O. Igbe, "Virtual Machine Introspection for Anomaly-Based Keylogger Detection," in *IEEE International Conference on High Performance Switching and Routing, HPSR*, 2020. doi: 10.1109/HPSR48589.2020.9098980.
- [32] R. Chanajitt, B. Pfahringer, H. M. Gomes, and V. Yogarajan, *Multiclass Malware Classification Using Either Static Opcodes or Dynamic API Calls*, vol. 13728 LNAI. 2022. doi: 10.1007/978-3-031-22695-3_30.
- [33] J. Singh, T. Gera, F. Ali, D. Thakur, K. Singh, and K.-S. Kwak, "Understanding research trends in android malware research using information modelling techniques," *Computers, Materials and Continua*, vol. 66, no. 3, pp. 2655–2670, 2021, doi: 10.32604/cmc.2021.014504.
- [34] Kaspersky Lab, "Android Mobile Security Threats," <https://www.kaspersky.com/resource-center/threats/mobile>.

- [35] AVG, “Malware And Virus Statistics 2024: The Trends You Need to Know About,” <https://www.avg.com/en/signal/malware-statistics>.
- [36] N. Penning, M. Hoffman, J. Nikolai, and Y. Wang, “Mobile malware security challeges and cloud-based detection,” in *2014 International Conference on Collaboration Technologies and Systems, CTS 2014*, 2014, pp. 181–188. doi: 10.1109/CTS.2014.6867562.
- [37] A. A. A. Samra, H. N. Qunoo, F. Al-Rubaie, and H. El-Talli, “A survey of static android malware detection techniques,” in *IEEE 7th Palestinian International Conference on Electrical and Computer Engineering, PICECE 2019*, 2019. doi: 10.1109/PICECE.2019.8747224.
- [38] K. Xu, Y. Li, and R. H. Deng, “ICCDetector: ICC-Based Malware Detection on Android,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1252–1264, 2016, doi: 10.1109/TIFS.2016.2523912.
- [39] G. Canfora, F. Mercaldo, E. Medvet, and C. A. Visaggio, “Detecting Android malware using sequences of system calls,” in *3rd International Workshop on Software Development Lifecycle for Mobile, DeMobile 2015 - Proceedings*, 2015, pp. 13–20. doi: 10.1145/2804345.2804349.
- [40] G. He, B. Xu, L. Zhang, and H. Zhu, “On-Device Detection of Repackaged Android Malware via Traffic Clustering,” *Security and Communication Networks*, vol. 2020, 2020, doi: 10.1155/2020/8630748.
- [41] V. Malik, S. K. Goyal, and N. Malik, “A hybrid model for android malware detection,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 12, pp. 2656–2662, 2019, doi: 10.35940/ijitee.K2250.1081219.
- [42] J. Zhao, X. Mo, and Q. Zheng, “A novel method of android malware detection based on ensemble learning algorithm,” in *Proceedings of 2018 the 8th International Workshop on Computer Science and Engineering, WCSE 2018*, 2018, pp. 531–538.
- [43] A. Dahiya, S. Singh, and G. Shrivastava, *Malware Detection Insights, Mechanisms and Future Perspectives for Android Applications*, vol. 1021 LNNS. 2024. doi: 10.1007/978-981-97-3591-4_31.
- [44] VirusTotal, “How it works,” <https://docs.virustotal.com/docs/how-it-works>.
- [45] C. Leka, C. Ntantogian, S. Karagiannis, E. Magkos, and V. S. Verykios, “A Comparative Analysis of VirusTotal and Desktop Antivirus Detection Capabilities,” in *13th International Conference on Information, Intelligence, Systems and Applications, IISA 2022*, 2022. doi: 10.1109/IISA56318.2022.9904382.
- [46] J. Charlton, P. Du, J.-H. Cho, and S. Xu, “Measuring Relative Accuracy of Malware Detectors in the Absence of Ground Truth,” in *Proceedings - IEEE Military Communications Conference MILCOM*, 2018, pp. 450–455. doi: 10.1109/MILCOM.2018.8599730.
- [47] A. Algaith, I. Gashi, B. Sobesto, M. Cukier, S. Haxhijaha, and G. Bajrami, “Comparing Detection Capabilities of AntiVirus Products: An Empirical Study with

- Different Versions of Products from the Same Vendors,” in *Proceedings - 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN-W 2016*, 2016, pp. 48–53. doi: 10.1109/DSN-W.2016.45.
- [48] X. Yuan, “PhD Forum: Deep Learning-Based Real-Time Malware Detection with Multi-Stage Analysis,” in *2017 IEEE International Conference on Smart Computing, SMARTCOMP 2017*, 2017. doi: 10.1109/SMARTCOMP.2017.7946997.
- [49] Z. Chen, X. Zhang, and S. Kim, “A learning-based static malware detection system with integrated feature,” *Intelligent Automation and Soft Computing*, vol. 27, no. 3, pp. 891–908, 2021, doi: 10.32604/IASC.2021.016933.
- [50] ReversingLabs, “REVERSINGLABS,” <https://www.reversinglabs.com/>.
- [51] MalwareBazaar, “About,” <https://bazaar.abuse.ch/about/>.
- [52] J. Oberheide, E. Cooke, and F. Jahanian, “CloudAV: N-version antivirus in the network cloud,” in *Proceedings of the 17th USENIX Security Symposium*, 2008, pp. 91–106.
- [53] I. Gashi, V. Stankovic, C. Leita, and O. Thonnard, “An experimental study of diversity with off-the-shelf antivirus engines,” in *Proceedings - 2009 8th IEEE International Symposium on Network Computing and Applications, NCA 2009*, 2009, pp. 4–11. doi: 10.1109/NCA.2009.14.
- [54] S. Khalid and F. B. Hussain, “Evaluating Opcodes for Detection of Obfuscated Android Malware,” in *4th International Conference on Artificial Intelligence in Information and Communication, ICAIIC 2022 - Proceedings*, 2022, pp. 44–49. doi: 10.1109/ICAIIIC54071.2022.9722669.
- [55] M. Y. Wong and D. Lie, “Tackling runtime-based obfuscation in Android with TIRO,” in *Proceedings of the 27th USENIX Security Symposium*, 2018, pp. 1247–1262.
- [56] I. You and K. Yim, “Malware obfuscation techniques: A brief survey,” in *Proceedings - 2010 International Conference on Broadband, Wireless Computing Communication and Applications, BWCCA 2010*, 2010, pp. 297–300. doi: 10.1109/BWCCA.2010.85.
- [57] A. Romano, D. Lehmann, M. Pradel, and W. Wang, “Wobfuscator: Obfuscating JavaScript Malware via Opportunistic Translation to WebAssembly,” in *Proceedings - IEEE Symposium on Security and Privacy*, 2022, pp. 1574–1589. doi: 10.1109/SP46214.2022.9833626.
- [58] D. Sharma and H. K. Verma, “Malware Signature and Behavior Performance Evaluation utilizing Packers,” in *2022 2nd Asian Conference on Innovation in Technology, ASIANCON 2022*, 2022. doi: 10.1109/ASIANCON55314.2022.9909111.
- [59] I. Martín, J. A. Hernández, and S. de los Santos, “Machine-Learning based analysis and classification of Android malware signatures,” *Future Generation Computer Systems*, vol. 97, pp. 295–305, 2019, doi: 10.1016/j.future.2019.03.006.
- [60] I. Martín, J. A. Hernández, S. De Los Santos, and A. Guzmán, “POSTER: Insights of antivirus relationships when detecting Android malware: A data analytics approach,”

in *Proceedings of the ACM Conference on Computer and Communications Security*, 2016, pp. 1778–1780. doi: 10.1145/2976749.2989038.

- [61] F. A. Bhuiyan, K. E. Brown, M. B. Sharif, Q. D. Johnson, and D. A. Talbert, “Assessing modality selection heuristics to improve multimodal deep learning for malware detection,” in *Proceedings of the 33rd International Florida Artificial Intelligence Research Society Conference, FLAIRS 2020*, 2020, pp. 434–437.
- [62] W. Gu, “A Multimodal Deep Network Model for Android Malware Detection Using Permission,” in *2021 IEEE International Conference on Electronic Technology, Communication and Information, ICETCI 2021*, 2021, pp. 63–67. doi: 10.1109/ICETCI53161.2021.9563414.
- [63] X. Li, Z. Zhao, Y. Tang, J. Zhang, C. Wu, and Y. Li, “An Android Malicious Application Detection Method with Decision Mechanism in the Operating Environment of Blockchain,” *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/3111540.
- [64] H. Yu, Y. Hu, Y. Gao, J. Xu, and M. Zhang, “Research on the technology of massive Android application data processing,” in *Proceedings of 2016 4th IEEE International Conference on Cloud Computing and Intelligence Systems, CCIS 2016*, 2016, pp. 99–103. doi: 10.1109/CCIS.2016.7790232.
- [65] M. Abdellatif, C. Talhi, A. Hamou-Lhadj, and M. Dagenais, “On the Use of Mobile GPU for Accelerating Malware Detection Using Trace Analysis,” in *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, 2015, pp. 42–46. doi: 10.1109/SRDSW.2015.18.
- [66] P. McNeil, S. Shetty, D. Guntu, and G. Barve, “SCREDDENT: Scalable Real-time Anomalies Detection and Notification of Targeted Malware in Mobile Devices,” in *Procedia Computer Science*, 2016, pp. 1219–1225. doi: 10.1016/j.procs.2016.04.254.
- [67] J. T. Ross, *Fuzzy Logic with Engineering Applications Third Edition*, 3rd ed. John Wiley & Sons, Ltd, 2010.
- [68] T. J. Ross, *FUZZY LOGIC WITH ENGINEERING APPLICATIONS, 3RD ED.* Wiley India Pvt. Limited, 2011. Accessed: Dec. 06, 2024. [Online]. Available: <https://books.google.co.id/books?id=mCV0CgAAQBAJ>
- [69] K. Slavyanov and R. Dimov, “APPLICATION OF FUZZY LOGIC IN CYBERSECURITY DECISION MAKING AND ANALYSIS AFTER A CYBER INCIDENT DETECTION,” *ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference*, vol. 2, pp. 259–263, Jun. 2024, doi: 10.17770/etr2024vol2.8022.
- [70] D. K. Jana and R. Ghosh, “Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security,” *Journal of Information Security and Applications*, vol. 40, pp. 173–182, Jun. 2018, doi: 10.1016/j.jisa.2018.04.002.
- [71] A. Borisova, “NETWORK ATTACK RECOGNITION USING FUZZY LOGIC,” *ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the*

International Scientific and Practical Conference, vol. 2, pp. 55–60, Jun. 2024, doi: 10.17770/etr2024vol2.8054.

- [72] O. Linda, M. Manic, T. Vollmer, and J. Wright, “Fuzzy logic based anomaly detection for embedded network security cyber sensor,” in *2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, IEEE, Apr. 2011, pp. 202–209. doi: 10.1109/CICYBS.2011.5949392.
- [73] O. Linda, M. Manic, J. Alves-Foss, and T. Vollmer, “Towards resilient critical infrastructures: Application of Type-2 Fuzzy Logic in embedded network security cyber sensor,” in *2011 4th International Symposium on Resilient Control Systems*, IEEE, Aug. 2011, pp. 26–32. doi: 10.1109/ISRCS.2011.6016083.
- [74] A. F. and K. M.-C. Shapiro, “Risk assessment applications of fuzzy logic,” *Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries*, vol. 390, 2015.
- [75] abuse.ch, “MalwareBazaar,” <https://bazaar.abuse.ch/>.
- [76] pypi.org, “malwarebazaar 0.2.7,” <https://pypi.org/project/malwarebazaar/>.
- [77] C. Camichel, “malware-bazaar /bazaar_download.py,” https://github.com/cocaman/malware-bazaar/blob/master/bazaar_download.py.
- [78] I. A. Hameed, “Using Gaussian membership functions for improving the reliability and robustness of students’ evaluation systems,” *Expert Syst Appl*, vol. 38, no. 6, pp. 7135–7142, Jun. 2011, doi: 10.1016/j.eswa.2010.12.048.
- [79] J. J. Sara and S. Hossain, “Static Analysis Based Malware Detection for Zero-Day Attacks in Android Applications,” in *2023 International Conference on Information and Communication Technology for Sustainable Development, ICICT4SD 2023 - Proceedings*, 2023, pp. 169–173. doi: 10.1109/ICICT4SD59951.2023.10303336.
- [80] D. Vanusha, S. Singh, A. K. Jha, and S. Delsi Robinsha, “SecuDroid : Android Malware Detection using ML classifier on Static Features,” in *Proceedings of the 2nd IEEE International Conference on Networking and Communications 2024, ICNWC 2024*, 2024. doi: 10.1109/ICNWC60771.2024.10537417.
- [81] G. Zhang, H. Li, Z. Chen, L. Peng, Y. Zhu, and C. Zhao, “AndroCreme: Unseen Android Malware Detection Based on Inductive Conformal Learning,” in *Proceedings - 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2021*, 2021, pp. 651–658. doi: 10.1109/TrustCom53373.2021.00097.
- [82] L. Gheorghe *et al.*, “Smart malware detection on Android,” *Security and Communication Networks*, vol. 8, no. 18, pp. 4254–4272, 2015, doi: 10.1002/sec.1340.
- [83] S. Millar, N. McLaughlin, J. Martinez del Rincon, and P. Miller, “Multi-view deep learning for zero-day Android malware detection,” *Journal of Information Security and Applications*, vol. 58, 2021, doi: 10.1016/j.jisa.2020.102718.