# Multi-Perspective Analysis of Binary-Classification Performance Evaluation Instruments

Gürol Canbek[1], Tugba Taskaya Temizel, and Seref Sagiroglu

***Appendix E:*** *Surveyed Android Malware Classification Studies*

Table E.1 lists the surveyed studies selected by the methodology described in Appendix D. The table, which is provided online at https://github.com/gurol/ptopi/AppendixE_TableE1.pdf, also shows which studies are applicable in the following analysis conducted in this study:

I. Included for performance-evaluation reporting analysis? (69 of 78)

II. Included for performance measures or metrics terminology usage? (55 of 78)

III. Included for alternative terms usage for individual metrics? (78 of 78)

**Table E.1** Surveyed studies and the applicable findings

| Nr | Study | I | II | III |
|---|---|---|---|---|
| S#1 | Aafer, Y., Du, W., & Yin, H. (2013). DroidAPIMiner: Mining API-level features for robust malware detection in Android. In *9th International Conference on Security and Privacy in Communication Networks (SecureComm)* (pp. 86–103). Sydney, NSW, Australia: Springer International Publishing | Yes | N/A | Yes |
| S#2 | Aonzo, S., Merlo, A., Migliardi, M., Oneto, L., & Palmieri, F. (2017). Low-resource footprint, data-driven malware detection on Android. *IEEE Transactions on Sustainable Computing*, *3782*, 1–1. https://doi.org/10.1109/TSUSC.2017.2774184. | Yes | Others | Yes |
| S#3 | Apvrille, L., & Apvrille, A. (2015). Identifying unknown android malware with feature extractions and classification techniques. In *14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (Vol. 1, pp. 182–189). https://doi.org/10.1109/Trustcom.2015.373 | Yes | N/A | Yes |
| S#4 | Arp, D., Spreitzenbarth, M., Hübner, M., Gascon, H., & Rieck, K. (2014). DREBIN: Effective and explainable detection of Android malware in your pocket. In *Network and Distributed System Security (NDSS) Symposium*. San Diego, California: Internet Society. https://doi.org/10.14722/ndss.2014.23247 | Yes | Others | Yes |
| S#5 | Aswini, A. M., & Vinod, P. (2014). Droid permission miner: Mining prominent permissions for Android malware analysis. In *The 5th International Conference on the Applications of Digital Information and Web Technologies (ICADIWT)* (pp. 81–86). Bangalore, India: IEEE. https://doi.org/10.1109/ICADIWT.2014.6814679 | Yes | Both | Yes |
| S#6 | Canfora, G., De Lorenzo, A., Medvet, E., Mercaldo, F., & Visaggio, C. A. (2015). Effectiveness of opcode ngrams for detection of multi family Android malware. In *10th International Conference on Availability, Reliability and Security (ARES)* (pp. 333–340). https://doi.org/10.1109/ARES.2015.57 | Yes | Metrics | Yes |
| S#7 | Canfora, G., Mercaldo, F., & Visaggio, C. A. (2013). A classifier of malicious Android applications. In *The 8th International Conference on Availability, Reliability and Security (ARES)* (pp. 607–614). Regensburg: IEEE. https://doi.org/10.1109/ARES.2013.80 | Yes | Metrics | Yes |
| S#8 | Cen, L., Gates, C., Si, L., & Li, N. (2015). A probabilistic discriminative model for Android malware detection with decompiled source code. *IEEE Transactions on Dependable and Secure Computing*, *12*(4), 400–412. https://doi.org/10.1109/TDSC.2014.2355839 | Yes | Metrics | Yes |
| S#9 | Damshenas, M., Dehghantanha, A., Choo, K.-K. R., & Mahmud, R. (2015). M0Droid: An Android behavioral-based malware detection model. *Journal of Information Privacy and Security*, *11*(3), 141–157. https://doi.org/10.1080/15536548.2015.1073510 | Yes | N/A | Yes |

[1] Corresponding author: gurol@canbek.com, METU, Informatics Institute, Ankara, Turkey

**Table E.1** Surveyed studies and the applicable findings (*continued*)

| Nr | Study | I | II | III |
|---|---|---|---|---|
| S#10 | Dash, S. K., Suarez-Tangil, G., Khan, S., Tam, K., Ahmadi, M., Kinder, J., & Cavallaro, L. (2016). DroidScribe: Classifying Android malware based on runtime behavior. In *IEEE Symposium on Security and Privacy Workshops (SPW)* (pp. 252–261). https://doi.org/10.1109/SPW.2016.25 | Yes | Metrics | Yes |
| S#11 | Demme, J., Maycock, M., Schmitz, J., Tang, A., Waksman, A., Sethumadhavan, S., & Stolfo, S. (2013). On the feasibility of online malware detection with performance counters. *ACM SIGARCH Computer Architecture News*, *41*(3), 559. https://doi.org/10.1145/2508148.2485970 | Yes | Metrics | Yes |
| S#12 | Demontis, A., Melis, M., Biggio, B., Maiorca, D., Arp, D., Rieck, K., … Roli, F. (2017). Yes, machine learning can be more secure! A case study on Android malware detection. *IEEE Transactions on Dependable and Secure Computing*, *PP*(99), 1–14. https://doi.org/10.1109/TDSC.2017.2700270 | Yes | Measures | Yes |
| S#13 | Deshotels, L., Notani, V., & Lakhotia, A. (2014). DroidLegacy: Automated familial classification of Android malware. In *3rd ACM SIGPLAN on Program Protection and Reverse Engineering Workshop (PPREW)* (pp. 1–12). San Diego, CA, USA: ACM. https://doi.org/10.1145/2556464.2556467 | Yes | Measures | Yes |
| S#14 | Dimjasevic, M., Atzeni, S., Ugrina, I., & Rakamaric, Z. (2016). Evaluation of Android malware detection based on system calls. In *International Workshop on Security and Privacy Analytics (IWSPA@CODASPY)* (pp. 1–8). New Orleans, LA: ACM. https://doi.org/10.1145/2875475.2875487 | Yes | Measures | Yes |
| S#15 | Du, Y. A. O., Wang, J., & Li, Q. I. (2017). An Android malware detection approach using community structures of weighted function call graphs. *IEEE Access*, *5*, 17478–17486. https://doi.org/10.1109/ACCESS.2017.2720160 | Yes | Metrics | Yes |
| S#16 | Elish, K. O., Shu, X., Yao, D., Ryder, B. G., & Jiang, X. (2015). Profiling user-trigger dependence for Android malware detection. *Computers and Security*, *49*(540), 255–273. https://doi.org/10.1016/j.cose.2014.11.001 | Yes | Others | Yes |
| S#17 | Fan, M., Liu, J., Luo, X., Chen, K., Tian, Z., Zheng, Q., & Liu, T. (2018). Android malware familial classification and representative sample selection via frequent subgraph analysis. *IEEE Transactions on Information Forensics and Security*, *13*(8), 1890–1905. https://doi.org/10.1109/TIFS.2018.2806891 | Yes | Metrics | Yes |
| S#18 | Fan, M., Liu, J., Wang, W., Li, H., Tian, Z., & Liu, T. (2017). DAPASA: Detecting Android piggybacked apps through sensitive subgraph analysis. *IEEE Transactions on Information Forensics and Security*, *12*(8), 1772–1785. https://doi.org/10.1109/TIFS.2017.2687880 | Yes | Metrics | Yes |
| S#19 | Feizollah, A., Badrul, N., & Salleh, R. (2017). AndroDialysis: Analysis of Android intent effectiveness in malware detection. *Computers & Security*, *65*, 121–134. https://doi.org/10.1016/j.cose.2016.11.007 | Yes | Others | Yes |
| S#20 | Feng, Y., Anand, S., Dillig, I., & Aiken, A. (2014). Apposcopy: Semantics-based detection of Android malware through static analysis. In *22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering (FSE 2014)* (pp. 576–587). Hong Kong: ACM. https://doi.org/10.1145/2635868.2635869 | Yes | N/A | Yes |
| S#21 | Garcia, J., Hammad, M., & Malek, S. (2018). Lightweight, obfuscation-resilient detection and family identification of Android malware. *ACM Transactions on Software Engineering and Methodology*, *26*(3), 1–29. https://doi.org/10.1145/3162625 | Yes | Metrics | Yes |
| S#22 | Gascon, H., Yamaguchi, F., Rieck, K., & Arp, D. (2013). Structural detection of Android malware using embedded call graphs. In *ACM Workshop on Artificial Intelligence and Security* (pp. 45–54). New York, New York, USA: ACM. https://doi.org/10.1145/2517312.2517315 | Yes | Measures | Yes |
| S#23 | Ge, H., Ting, L., Hang, D., Hewei, Y., & Miao, Z. (2014). Malicious code detection for Android using instruction signatures. In *8th International Symposium on Service Oriented System Engineering (SOSE)* (pp. 332–337). Oxford, UK: IEEE. https://doi.org/10.1109/SOSE.2014.48 | Yes | N/A | Yes |
| S#24 | Glodek, W., & Harang, R. (2013). Rapid permissions-based detection and analysis of mobile malware using random decision forests. In *Military Communications Conference (MILCOM)* (pp. 980–985). San Diego, CA: IEEE. https://doi.org/10.1109/MILCOM.2013.170 | Yes | N/A | Yes |
| S#25 | Ham, H.-S., & Choi, M.-J. (2013). Analysis of Android malware detection performance using machine learning classifiers. In *International Conference on ICT Convergence (ICTC)* (pp. 490–495). Jeju: IEEE. https://doi.org/10.1109/ICTC.2013.6675404 | Yes | Metrics | Yes |
| S#26 | Jerome, Q., Allix, K., State, R., & Engel, T. (2014). Using opcode-sequences to detect malicious Android applications. In *Communication and Information Systems Security Symposium (IEEE ICC 2014)* (pp. 914–919). https://doi.org/10.1109/ICC.2014.6883436 | Yes | Both | Yes |

**Table E.1** Surveyed studies and the applicable findings (*continued*)

| Nr | Study | I | II | III |
|---|---|---|---|---|
| S#27 | Kirubavathi, G., & Anitha, R. (2018). Structural analysis and detection of android botnets using machine learning techniques. *International Journal of Information Security*, *17*(2), 153–167. https://doi.org/10.1007/s10207-017-0363-3 | Yes | Both | Yes |
| S#28 | Li, J., Sun, L., Yan, Q., Li, Z., Srisa-an, W., & Ye, H. (2018). Significant permission identification for machine learning based Android malware detection. *IEEE Transactions on Industrial Informatics*, *14*(7), 3216–3225. https://doi.org/10.1109/TII.2017.2789219 | Yes | Both | Yes |
| S#29 | Liang, S., & Du, X. (2014). Permission-combination-based scheme for Android mobile malware detection. In *IEEE International Conference on Communications (ICC)* (pp. 2301–2306). Sydney, NSW, Australia: IEEE. https://doi.org/10.1109/ICC.2014.6883666 | Yes | N/A | Yes |
| S#30 | Liu, X., & Liu, J. (2014). A two-layered permission-based Android malware detection scheme. In *2nd International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* (pp. 142–148). Oxford, UK: IEEE. https://doi.org/10.1109/MobileCloud.2014.22 | Yes | Metrics | Yes |
| S#31 | Lu, Y., Zulie, P., Jingju, L., & Yi, S. (2013). Android malware detection technology based on improved Bayesian classification. In *The 3rd International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC)* (pp. 1338–1341). Shenyang: IEEE. https://doi.org/10.1109/IMCCC.2013.297 | Yes | N/A | Yes |
| S#32 | Mahindru, A., & Singh, P. (2017). Dynamic permissions-based Android malware detection using machine learning techniques. In *10th Innovations in Software Engineering Conference (ISEC)* (pp. 202–210). Jaipur, India: ACM. https://doi.org/10.1145/3021460.3021485 | Yes | Both | Yes |
| S#33 | Martinelli, F., Mercaldo, F., & Saracino, A. (2017). BRIDEMAID: An hybrid tool for accurate detection of Android malware. In *Asia Conference on Computer and Communications Security (ASIA CCS)* (pp. 899–901). Abu Dhabi, United Arab Emirates: ACM. https://doi.org/10.1145/3052973.3055156 | Yes | N/A | Yes |
| S#34 | Matsudo, T., Kodama, E., Wang, J., & Takata, T. (2012). A proposal of security advisory system at the time of the installation of applications on Android OS. In *International Conference on Network-Based Information Systems* (pp. 261–267). Melbourne, VIC: IEEE. https://doi.org/10.1109/NBiS.2012.110 | Yes | N/A | Yes |
| S#35 | Meng, G., Xue, Y., Xu, Z., Liu, Y., Zhang, J., & Narayanan, A. (2016). Semantic modelling of Android malware for effective malware comprehension, detection, and classification. In *25th International Symposium on Software Testing and Analysis (ISSTA)* (pp. 306–317). Saarbrücken, Germany: ACM. https://doi.org/10.1145/2931037.2931043 | Yes | Others | Yes |
| S#36 | Milosevic, N., Dehghantanha, A., & Choo, K.-K. R. (2017). Machine learning aided Android malware classification. *Computers and Electrical Engineering*, *61*, 266–274. https://doi.org/10.1016/j.compeleceng.2017.02.013 | Yes | Both | Yes |
| S#37 | Muttik, I., Yerima, S. Y., & Sezer, S. (2015). High accuracy Android malware detection using ensemble learning. *IET Information Security*, *9*(6), 313–320. https://doi.org/10.1049/iet-ifs.2014.0099 | Yes | Metrics | Yes |
| S#38 | Narayanan, A., Chandramohan, M., Chen, L., & Liu, Y. (2017). Context-aware, adaptive, and scalable Android malware detection through online learning. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *1*(3), 157–175. https://doi.org/10.1109/TETCI.2017.2699220 | Yes | Metrics | Yes |
| S#39 | Narudin, F. A., Feizollah, A., Anuar, N. B., & Gani, A. (2016). Evaluation of machine learning classifiers for mobile malware detection. *Soft Computing*, *20*(1), 343–357. https://doi.org/10.1007/s00500-014-1511-6 | Yes | Both | Yes |
| S#40 | Pan, J. S., Yang, C. N., & Lin, C. C. (2013). Performance evaluation on permission-based detection for Android malware. *Advances in Intelligent Systems & Applications, Smart Innovation, Systems and Technologies (SIST)*, *21*, 111–120. https://doi.org/10.1007/978-3-642-35473-1 | Yes | Metrics | Yes |
| S#41 | Peiravian, N., & Zhu, X. (2013). Machine learning for Android malware detection using permission and API calls. In *IEEE 25th International Conference on Tools with Artificial Intelligence (ICTAI)* (pp. 300–305). Herndon, VA: IEEE. https://doi.org/10.1109/ICTAI.2013.53 | Yes | N/A | Yes |
| S#42 | Rahman, M. (2013). DroidMLN: A Markov logic network approach to detect android malware. In *Proceedings - 2013 12th International Conference on Machine Learning and Applications, ICMLA 2013* (Vol. 2, pp. 166–169). https://doi.org/10.1109/ICMLA.2013.184 | Yes | N/A | Yes |
| S#43 | Rahman, M., Rahman, M., Carbunar, B., & Chau, D. H. (2017). Search rank fraud and malware detection in Google Play. *IEEE Transactions on Knowledge and Data Engineering*, *29*(6), 1329–1342. https://doi.org/10.1109/TKDE.2017.2667658 | Yes | N/A | Yes |

**Table E.1** Surveyed studies and the applicable findings (*continued*)

| Nr | Study | I | II | III |
|---|---|---|---|---|
| S#44 | Sahs, J., & Khan, L. (2012). A machine learning approach to Android malware detection. In *European Intelligence and Security Informatics Conference (EISIC)* (pp. 141–147). Odense: IEEE. https://doi.org/10.1109/EISIC.2012.34 | Yes | Measures | Yes |
| S#45 | Sanz, B., Santos, I., Laorden, C., Ugarte-Pedrero, X., Bringas, P. G., & Alvarez, G. (2013). PUMA: Permission usage to detect malware in Android. In *International Joint Conference CISIS-ICEUTE-SOCO Special Sessions* (pp. 289–298). Ostrava, Czech Republic: Springer Berlin Heidelberg. | Yes | Others | Yes |
| S#46 | Sanz, B., Santos, I., Laorden, C., Ugarte-Pedrero, X., Nieves, J., Bringas, P. G., & Marañón, G. Á. (2013). MAMA: Manifest analysis for malware detection in Android. *Cybernetics and Systems*, *44*(6–7), 469–488. https://doi.org/10.1080/01969722.2013.803889 | Yes | Both | Yes |
| S#47 | Sen, S., Aysan, A. I., & Clark, J. A. (2018). SAFEDroid: Using structural features for detecting Android malwares. In *Security and Privacy in Communication Networks (SecureComm 2017) - Workshop on Security and Privacy on Internet of Things (SePrIoT)* (pp. 255–270). Niagara Falls, Canada: Springer International Publishing. https://doi.org/10.1007/978-3-319-78816-6_18 | Yes | Metrics | Yes |
| S#48 | Sheen, S., Anitha, R., & Natarajan, V. (2015). Android based malware detection using a multifeature collaborative decision fusion approach. *Neurocomputing*, *151*(P2), 905–912. https://doi.org/10.1016/j.neucom.2014.10.004 | Yes | Measures | Yes |
| S#49 | Shen, F., Vecchio, J. Del, Mohaisen, A., Ko, S. Y., & Ziarek, L. (2017). Android malware detection using complex-flows. In *37th International Conference on Distributed Computing Systems (ICDCS)* (pp. 2430–2437). Atlanta, GA, USA: IEEE. https://doi.org/10.1109/ICDCS.2017.190 | Yes | Metrics | Yes |
| S#50 | Shen, Z., Hsu, C.-W., & Shieh, S. W. (2017). Security semantics modeling with progressive distillation. *IEEE Transactions on Mobile Computing*, *16*(11), 3196–3208. https://doi.org/10.1109/TMC.2017.2690425 | Yes | N/A | Yes |
| S#51 | Suarez-Tangil, G., Dash, S. K., Holloway, R., Ahmadi, M., Giacinto, G., Kinder, J., & Cavallaro, L. (2017). DroidSieve: Fast and accurate classification of obfuscated Android malware. In *7th ACM Conference on Data and Application Security and Privacy (CODASPY)* (pp. 309–320). Scottsdale, Arizona: ACM. https://doi.org/10.1145/3029806.3029825 | Yes | Metrics | Yes |
| S#52 | Talha, K. A., Alper, D. I., & Aydin, C. (2015). APK Auditor: Permission-based Android malware detection system. *Digital Investigation*, *13*, 1–14. https://doi.org/10.1016/j.diin.2015.01.001 | Yes | N/A | Yes |
| S#53 | Tao, G., Zheng, Z., Guo, Z., & Lyu, M. R. (2017). MalPat: Mining patterns of malicious and benign Android apps via permission-related APIs. *IEEE Transactions on Reliability*, *67*(1), 355–369. https://doi.org/10.1109/TR.2017.2778147 | Yes | Both | Yes |
| S#54 | Tian, K., Yao, D., Ryder, B. G., & Tan, G. (2016). Analysis of code heterogeneity for high-precision classification of repackaged malware. In *IEEE Symposium on Security and Privacy Workshops (SPW)* (pp. 262–271). San Jose, CA, USA: IEEE. https://doi.org/10.1109/SPW.2016.33 | Yes | N/A | Yes |
| S#55 | Tong, F., & Yan, Z. (2017). A hybrid approach of mobile malware detection in Android. *Journal of Parallel and Distributed Computing*, *103*, 22–31. https://doi.org/10.1016/j.jpdc.2016.10.012 | Yes | N/A | Yes |
| S#56 | Wang, S., Yan, Q., Chen, Z., Yang, B., Zhao, C., & Conti, M. (2018). Detecting Android malware leveraging text semantics of network flows. *IEEE Transactions on Information Forensics and Security*, *13*(5), 1096–1109. https://doi.org/10.1109/TIFS.2017.2771228 | Yes | Both | Yes |
| S#57 | Wang, W., Li, Y., Wang, X., Liu, J., & Zhang, X. (2018). Detecting Android malicious apps and categorizing benign apps with ensemble of classifiers. *Future Generation Computer Systems*, *78*, 987–994. https://doi.org/10.1016/j.future.2017.01.019 | Yes | Measures | Yes |
| S#58 | Wang, W., Wang, X., Feng, D., Liu, J., Han, Z., & Zhang, X. (2014). Exploring permission-induced risk in Android applications for malicious application detection. *IEEE Transactions on Information Forensics and Security*, *9*(11), 1828–1842. https://doi.org/10.1109/TIFS.2014.2353996 | Yes | Measures | Yes |
| S#59 | Wei, T.-E., Mao, C.-H., Jeng, A. B., Lee, H.-M., Wang, H. T., & Wu, D.-J. (2012). Android malware detection via a latent network behavior analysis. In *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012* (pp. 1251–1258). https://doi.org/10.1109/TrustCom.2012.91 | Yes | Metrics | Yes |
| S#60 | Wu, D.-J., Mao, C.-H., Wei, T.-E., Lee, H.-M., & Wu, K.-P. (2012). DroidMat: Android malware detection through manifest and API calls tracing. In *The 7th Asia Joint Conference on Information Security (Asia JCIS)* (pp. 62–69). Tokyo: IEEE. https://doi.org/10.1109/AsiaJCIS.2012.18 | Yes | Metrics | Yes |

**Table E.1** Surveyed studies and the applicable findings (*continued*)

| Nr | Study | I | II | III |
|---|---|---|---|---|
| S#61 | Wu, W.-C., & Hung, S.-H. (2014). DroidDolphin: A dynamic Android malware detection framework using big data and machine learning. In *Conference on Research in Adaptive and Convergent Systems (RACS)* (pp. 247–252). Towson, Maryland: ACM. https://doi.org/10.1145/2663761.2664223 | Yes | Both | Yes |
| S#62 | Xiao, X., Wang, Z., Li, Q., Xia, S., & Jiang, Y. (2017). Back-propagation neural network on Markov chains from system call sequences: A new approach for detecting Android malware with system call sequences. *IET Information Security*, *11*(1), 8–15. https://doi.org/10.1049/iet-ifs.2015.0211 | Yes | Others | Yes |
| S#63 | Xu, K., Li, Y., & Deng, R. H. (2016). ICCDetector: ICC-based malware detection on Android. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1252–1264. https://doi.org/10.1109/TIFS.2016.2523912 | Yes | Metrics | Yes |
| S#64 | Yang, C., Xu, Z., Gu, G., Yegneswaran, V., & Porras, P. A. (2014). DroidMiner: Automated mining and characterization of fine-grained malicious behaviors in Android applications. In *European Symposium on Research in Computer Security (ESORICS)* (pp. 163–182). Wrocław, Poland: Springer. https://doi.org/10.1007/978-3-319-11203-9_10 | Yes | Metrics | Yes |
| S#65 | Yerima, S. Y., Sezer, S., & McWilliams, G. (2014). Analysis of Bayesian classification-based approaches for Android malware detection. *IET Information Security*, *8*(1), 25–36. https://doi.org/10.1049/iet-ifs.2013.0095 | Yes | Both | Yes |
| S#66 | Yerima, S. Y., Sezer, S., & Muttik, I. (2014). Android malware detection using parallel machine learning classifiers. In *The 8th International Conference on Next Generation Mobile Apps, Services and Technologies (NGMAST)* (pp. 37–42). Oxford, United Kingdom: IEEE. https://doi.org/10.1109/NGMAST.2014.23 | Yes | Metrics | Yes |
| S#67 | Yerima, S. Y., Sezer, S., McWilliams, G., & Muttik, I. (2013). A new Android malware detection approach using Bayesian classification. In *27th International Conference on Advanced Information Networking and Applications (AINA)* (pp. 121–128). Barcelona, Spain: IEEE. https://doi.org/10.1109/AINA.2013.88 | Yes | Both | Yes |
| S#68 | Yuan, Z., Lu, Y., & Xue, Y. (2016). Droiddetector: Android malware characterization and detection using deep learning. *Tsinghua Science and Technology*, *21*(1), 114–123. https://doi.org/10.1109/TST.2016.7399288 | Yes | N/A | Yes |
| S#69 | Yuan, Z., Lu, Y., Wang, Z., & Xue, Y. (2014). Droid-Sec: Deep learning in Android malware detection. In *ACM Conference on SIGCOMM* (pp. 371–372). Chicago, Illinois, USA: ACM. https://doi.org/10.1145/2619239.2631434 | Yes | Others | Yes |
| S#70 | Abawajy, J., & Kelarev, A. (2017). Iterative classifier fusion system for the detection of Android malware. *IEEE Transactions on Big Data*, *5*(3), 1–1. https://doi.org/10.1109/TBDATA.2017.2676100 | N/A | Both | Yes |
| S#71 | Azmoodeh, A., Dehghantanha, A., & Choo, K.-K. R. (2018). Robust malware detection for Internet Of (Battlefield) Things devices using deep eigenspace learning. *IEEE Transactions on Sustainable Computing*, *3782*(c), 1–1. https://doi.org/10.1109/TSUSC.2018.2809665 | N/A | Metrics | Yes |
| S#72 | Dini, G., Martinelli, F., Matteucci, I., Petrocchi, M., Saracino, A., & Sgandurra, D. (2016). Risk analysis of Android applications: A user-centric solution. *Future Generation Computer Systems*, *80*, 505–518. https://doi.org/10.1016/j.future.2016.05.035 | N/A | N/A | Yes |
| S#73 | Grace, M., Zhou, Y., Zhang, Q., Zou, S., & Jiang, X. (2012). RiskRanker: Scalable and accurate zero-day Android malware detection categories and subject descriptors. In *International Conference on Mobile Systems, Applications, and Services (MobiSys)* (pp. 281–294). Low Wood Bay, Lake District: ACM. https://doi.org/10.1145/2307636.2307663 | N/A | Others | Yes |
| S#74 | Peng, H., Gates, C., Sarma, B., Li, N., Qi, Y., Potharaju, R., Nita-Rotaru, C., Molloy, I. (2012). Using probabilistic generative models for ranking risks of Android apps. In *19th Conference on Computer and Communications Security (CCS)* (pp. 241–252). New York, New York, USA: ACM. https://doi.org/10.1145/2382196.2382224 | N/A | N/A | Yes |
| S#75 | Sarma, B., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., & Molloy, I. (2012). Android permissions: A perspective combining risks and benefits. In *17th Symposium on Access Control Models and Technologies (SACMAT)* (pp. 13–22). New York, New York, USA: ACM. https://doi.org/10.1145/2295136.2295141 | N/A | N/A | Yes |
| S#76 | Schmidt, A., Bye, R., Schmidt, H., Clausen, J., & Kiraz, O. (2009). Static analysis of executables for collaborative malware detection on Android. In *IEEE International Conference on Communications* (pp. 1–5). Dresden, Germany: IEEE. https://doi.org/10.1109/ICC.2009.5199486 | N/A | Others | Yes |
| S#77 | Sun, M., Li, X., Lui, J., & Ma, R. (2017). MONET: A user-oriented behavior-based malware variants detection system for Android. *IEEE Transactions on Information Forensics and Security*, *12*(5), 1103–1112. https://doi.org/10.1109/TIFS.2016.2646641 | N/A | N/A | Yes |
| S#78 | Zhang, M., Duan, Y., Yin, H., & Zhao, Z. (2014). Semantics-aware Android malware classification using weighted contextual API dependency graphs. In *ACM SIGSAC* | N/A | N/A | Yes |

**Table E.1** Surveyed studies and the applicable findings (*continued*)

| Nr | Study | I | II | III |
|---|---|---|---|---|
| | *Conference on Computer and Communications Security (CCS)* (pp. 1105–1116). Scottsdale, Arizona, USA: ACM. https://doi.org/10.1145/2660267.2660359 | | | |