[12] A. Saracino, D. Sgandurra, G. Dini, and F. Martinelli, “MADAM: Effective and Efficient Behavior-based Android Malware Detection and Prevention,” IEEE Trans. Dependable Secur. Comput., vol. 15, no. 1, pp. 83–97, Jan. 2016.
[13] S. Y. Yerima, S. Sezer, and I. Muttik, “High accuracy android malware detection using ensemble learning,” IET Inf. Secur., vol. 9, no. 6, pp. 313–320, Nov. 2015.
[14] Z. Wang, J. Cai, S. Cheng, and W. Li, “DroidDeepLearner: Identifying Android malware using deep learning,” in 37th IEEE Sarnoff Symposium, Sarnoff 2016, 2017, pp. 160–165.
[15] Kamesh and N. S. Priya, "Security Enhancement of Authenticated RFID Generation," International Journal of Applied Engineering Research (IJAER), vol. 9, no. 22, pp. 5968-5974, 2014.
[16] J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-An, and H. Ye, “Significant Permission Identification for Machine-Learning-Based Android Malware Detection,” IEEE Trans. Ind. Informatics, vol. 14, no. 7, pp. 3216–3225, Jul. 2018.
[17] D. Li, Z. Wang, L. Li, Z. Wang, Y. Wang, and Y. Xue, “FgDetector: Fine-Grained Android Malware Detection,” in Proceedings - 2017 IEEE 2nd International Conference on Data Science in Cyberspace, DSC 2017, 2017, pp. 311–318.
[18] M. Mohd Saudi and A. Husainiamer, “Mobile Malware Classification via System Calls and Permission for GPS Exploitation,” Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 6, pp. 277–283, 2017.
[19] P. Burnap, R. French, F. Turner, and K. Jones, “Malware classification using self organising feature maps and machine activity data,” Comput. Secur., vol. 73, pp. 399–410, Mar. 2018.
[20] S. Wang, Q. Yan, Z. Chen, B. Yang, C. Zhao, and M. Conti, “Detecting Android Malware Leveraging Text Semantics of Network Flows,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 5, pp. 1096–1109, May 2018.
[21] Z. Abdullah and M. M. Saudi, “RAPID-Risk assessment of android permission and application programming interface (API) call for android botnet,” Int. J. Eng. Technol., vol. 7, no. 4, pp. 49–54, 2018.
[22] S. Chen et al., “Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach,” Comput. Secur., vol. 73, pp. 326–344, Mar. 2018.
[23] S. Y. Yerima and S. Sezer, “DroidFusion: A Novel Multilevel Classifier Fusion Approach for Android Malware Detection,” IEEE Trans. Cybern., vol. 49, no. 2, pp. 453–466, Jan. 2018.
[24] M. Abou-Ghali and J. Stiban, “Regulation of ceramide channel formation and disassembly: Insights on the initiation of apoptosis,” Saudi J. Biol. Sci., vol. 22, no. 6, pp. 760–772, Nov. 2015.
[25] D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon, and K. Rieck, “Drebin: Effective and Explainable Detection of Android Malware in Your Pocket,” in Network and Distributed System Security Symposium(NDSS), 2014, pp. 1–15.
[26] M. Yusof, M. M. Saudi, and F. Ridzuan, “A new mobile botnet classification based on permission and API calls,” in Proceedings - 2017 7th International Conference on Emerging Security Technologies, EST 2017, 2017, pp. 122–127.
[27] Z. Li, L. Sun, Q. Yan, W. Srisa-An, and Z. Chen, “DroidClassifier: Efficient adaptive mining of application-layer header for classifying android malware,” in Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 2017, vol. 198 LNICST, pp. 597–616.
[28] M. Lindorfer, M. Neugschwandtner, L. Weichselbaum, Y. Fratantonio, V. Van Der Veen, and C. Platzer, “ANDRUBIS - 1,000,000 Apps Later: A View on Current Android Malware Behaviors,” in Proceedings - 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS 2014, 2016, pp. 3–17.
[29] R. Sihwail, K. Omar, and K. A. Z. Ariffin, “A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis,” Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 4–2, pp. 1662–1671, Sep. 2018.