IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

Malicious Android Application Detection Method using Machine Learning

Divya Chaudhari[1], Arati Chaure[2], Shreyash Dhadke[3], Tushar Dhanawate[4], Prof. Shraddha Shirsath[5]
Students, Department of Computer Engineering[1,2,3,4]
Professor, Department of Computer Engineering[5]
Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Abstract: *With the increasing popularity of the Android platform, we have seen the rapid growth of malicious Android applications recently. Considering that the heavy use of applications on mobile phones such as games, emails, and social network services has become a crucial part of our daily life, we have become more vulnerable to malicious applications running on mobile devices. This paper demonstrates on the problem of detecting malicious applications in the mobile internet, which is of great importance for personal information security and privacy security. We convert the android internet malicious application detection problem to a classification problem, and utilize the SVM classifier to solve it. Finally, we conduct an experiment to test the performance of the proposed method. Experimental results that the proposed can detect android internet malicious application with higher accuracy, true positive rate, and lower false positive rate.*

Keywords: SVM, Android internet, malicious application

REFERENCES

[1]. G. Jacob, H. Debar, and E. Filiol, "Behavior detection of mal ware: from a survey toward an established taxonomy", ComputVirol, pp: 251-226, 2008.
[2]. M. Schultz, E. Eskin, E. Zadok and S. Stolfo, "Data mining methods for detection of new malicious executables", Proceedings of the 2001 IEEE Symposium on Security and Privacy, Washington : IEEE Computer Society, pp. 38-49, 2001.
[3]. P. Joshi, C. Jindal, M. Chowkwale, R. Shethia, S. A. Shaikh, and D. Ved, "Protego: A passive intrusion detection system for android smartphones," in 2016 International Conference on Computing, Analytics and Security Trends (CAST), Dec 2016, pp. 232–237.
[4]. A. Kapratwar, F. Di Troia, and M. Stamp, "Static and dynamic analysis of android malware," pp. 653–662, 01 2017.
[5]. Raja, L.; Baboo, S.S. An overview of MANET: Applications, attacks and challenges. Int. J. Comput. Sci. Mob. Comput. 2014, 3, 408–417
[6]. Sivakami, R.; Nawaz, G.K. Secured communication for MANETS in military. In Proceedings of the 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET), Tirunelveli, Tamilnadu, India, 18–19 March 2011; pp. 146–151.
[7]. Cho, J.-H.; Swami, A.; Chen, R. A survey on trust management for mobile ad hoc networks.IEEE CommunSurv. Tutor. 2010, 13, 562–583.
[8]. VenkataRaoMaddumala, (2020), "Enhanced Morphological Operations for Improving the Pixel Intensity Level", International Journal of Advanced Science and Technology, Vol. 29, No. 03, (2020), pp. 9191 - 9201.
[9]. Schweitzer, N.; Stulman, A.; Shabtai, A.; Margalit, R.D. Mitigating denial of service attacks in olsr protocol using fictitious nodes. IEEE Trans. Mob. Comput. 2015, 15, 163–172.
[10]. Bharathi C R ,(2018),"Multi-mode Routing Algorithm with Cryptographic Techniques and Reduction of Packet Drop using 2ACK scheme in MANETs", Smart Intelligent Computing and Applications, Vo1.1, pp.649-658. DOI: 10.1007/978-981-13-1921- 1_63.