Journal of Advances in Science and Technology
Vol. 18, Issue No. 2, September–2021, ISSN 2230-9659

A review on multimodal malware detection techniques for android IOT devices

Baviskar Pallavi Vasudev[1]*, Dr. Guddi Singh[2]

[1] Phd Student. Kalinga University, Raipur

[2] Phd Guide, Kalinga University, Raipur

Abstract - Nowadays there is a huge applications of IOT and used in day to day life. There is a revolution in the world due to the ingress of Internet of Things (IoT) which advances applications in various aspects of life considering sensing, healthcare, remote monitoring, etc. The android device and application work close enough to realize dreams of IOT. Also there is a quick increase in threats and malware attacks on Android - based devices. Furthermore, due to wide utilization of the Android platform in the IoT devices generates a task demanding of securing malware activities. This paper looks into the IOT devices with malicious software detection methods. A review on multimodal malware detection is presented.

Keywords - Malware, IoT, Multimodal malware, Android, Malware detection and Machine Learning

----------X----------

1. INTRODUCTION

Different devices are integrated through a network in IOT environment due to the advancement of intelligence services.. IoT technology, which is used for convenience of life and for various purposes, has become a target of malicious users [1] as it enables high performance computing and processing of large tasks.

Internet of Things (IoT) and the cloud computing applications facilitate complex and intellectual services Which make the life of everyone easy. The application should become familiar its actions to the surroundings. General architecture of IOT environment is shown in fig. 1.

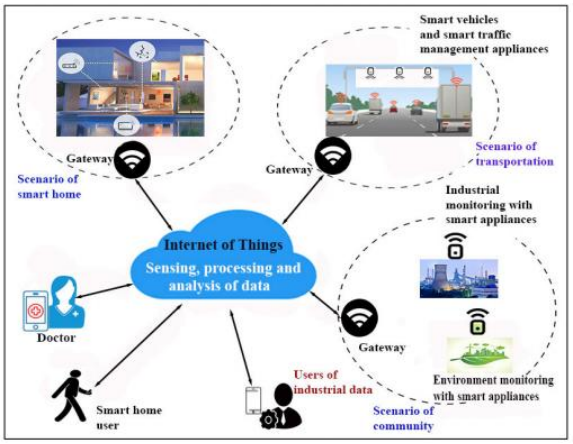

Figure 1: General Architecture of IOT Environment

Recently, the development of intelligent services provides an IoT environment in which various devices are integrated through a network. IoT technology, which is used for convenience of life and for various purposes, has become a target of malicious users [1] as it enables high performance computing and processing of large tasks.

Most of the devices in a shared IoT network are based on the Android platform due to flexibility, robustness and hardware support, which is pivotal for sensors interface. It is important to defend against various attacks such as spoofing attacks, denial of service (DoS) attacks, jamming, and eavesdropping, which are vulnerable to numerous IoT - based services for different purposes. There is a need for privacy protection to prepare for vulnerabilities in accessibility features that allow quick and easy access to IoT's miniaturized devices. Beyond security for IoT devices, strong defenses against environmentally oriented malicious attacks such as home automation and smart grids / cities are also required. To minimize malicious attacks in the IoT environment, intelligent IoT security technology using machine learning, unsupervised learning, and reinforcement learning is needed [2]. Figure 2 shows the IoT based android devices.

Figure 2: IOT based Android devices

Furthermore, the Android devices are attractive target for hackers due to extensive use of the Android platform in IoT devices . The purpose - built, diverse IoT environment is a malicious attack that results from a variety of external vulnerabilities, including a single device, network, firmware update, and new user connections. Existing studies can detect malicious behavior in a single device or feature - based detection of malicious code that has already been analyzed. However, it is very difficult to detect attacks by the association of different behaviors occurring in various environments. For this, learning process is necessary to classify ambiguous act into malicious act and non - malignant act to detect malicious attack. In other words, we need to extract features that can define malicious behavior and construct a learning model that can learn the behavior .

The mobile phone has become crucial these years with the developing number of clients of cell phones tablets and with their expanding number of multifaceted nature and capacities. Current cell phones offer a large portion of the applications and services that are executed by PCs. In the meantime, there is various security dangers focus on the cell phones. The usual approach for malware identification dependent on signature is generally utilized both belong to Android gadgets and PCs by separating the signatures from APK and contrasting with signature which is malicious in the infection database, nonetheless, such methodology is restricted to recognize obscure malwares that are not available in the infection database.

The predominance of malevolent applications in cell phones can be distinguished through various sorts of examination like static, dynamic and hybrid methods. In static methodology, we gather a lot of apps and recognize it for dangerous signs. In dynamic methodology, we test for pernicious records while executing on Android system. When both of these futures are combined, termed it as hybrid methodology.

The great deal of researches in the field of identification of malwares has been done in the past. The tale dynamic examination strategy termed Component Traversals is recommended that could naturally run the source code schedules of every Android apps as totally as could be expected under the circumstances. In light of the extricated system calls of Linux, those further develop the weighted coordinated diagrams and afterward apply a profound learning structure laying on the chart based highlights for recently obscure Android malware identification. Be that as it may, Android applications are ran in simulator and from such information, framework calls are extricated. In such situation, few malwares can distinguish whether they run on genuine gadget or emulator and as needs be transform the usefulness. Because of which, some malwares can't be recognized from such strategies.

2. LITERATURE REVIEW

An overview of Android malware detection is explained [8]. The Analysis is carried out for 4years from 2010 to 2014.The android security enforcement is discussed along with threat and security related issues. Different machine learning methods applied for the detection of malware [9] . The ML methods are Random Forest, Simple Logistic, Naïve Bayes, Decision Tree, and k - star. Simple Logistics performs better in comparable to others.

A method consisting of PCA and deep neural network is explained [10] .The feature selection is carried out by PCA. An experiment was performed on 1, 20,000 Android apps and achieved the detection rate of 94%. To find the malware Hidden Markov Model is used [11]. This is done by dynamic analysis. classification algorithms were trained by using API calls as features and compared the results of static and dynamic analysis. Experimental results show that dynamic analysis.

Late years, with the fast improvement of cell phones, Android is turning out to be increasingly well known. Android has been increasingly more fundamental along its open source properties and favourable circumstances of free in day by day life belong to us. In any case, the quantity of malicious programs is likewise developing quickly. Along these lines, how to identify the Android spyware with increased exact rate will be a hot challenge.

The mobile phone has become crucial these years with the developing number of clients of cell phones tablets and with their expanding number of multifaceted nature and capacities. Current cell phones offer a large portion of the applications and services that are executed by PCs. In the meantime, there is various security dangers focus on the cell phones. The usual approach for malware identification dependent on signature is generally utilized both belong to Android gadgets and PCs by separating the signatures from APK and contrasting with signature which is malicious in the infection database, nonetheless, such methodology is restricted to recognize obscure malwares that are not available in the infection database.

The predominance of malevolent applications in cell phones can be distinguished through various sorts of examination like static, dynamic and hybrid methods. In static methodology, we gather a lot of apps and recognize it for dangerous signs. In dynamic methodology, we test for pernicious records while executing on Android system. When both of these futures are combined, termed it as hybrid methodology.

The great deal of researches in the field of identification of malwares has been done in the past. The tale dynamic examination strategy termed Component Traversals is recommended that could naturally run the source code schedules of every Android apps as totally as could be expected under the circumstances. In light of the extricated system calls of Linux, those further develop the weighted coordinated diagrams and afterward apply a profound learning structure laying on the chart based highlights for recently obscure Android malware identification. Be that as it may, Android applications are ran in simulator and from such information, framework calls are extricated. In such situation, few malwares can distinguish whether they run on genuine gadget or emulator and as needs be transform the usefulness. Because of which, some malwares can't be recognized from such strategies.

According to the proposal in [12], an element vector is removed out of Android Manifest document, that joins the permission data and the segment data of the Android app. Joined with the classifications algorithms such as Naive Bayes, this methodology proposes a noxious app recognition strategy dependent on Android Manifest record data. This methodology is a static technique for malware identification which implies that apps are not executed or investigated at execution time for conduct examination. Hence, it can't distinguish any novice malware that are equipped for repackaging and confusion to sidestep internal techniques belong to them.

The work [13] utilizes a robotized feature - dependent static investigation strategy to recognize noxious versatile applications on Android gadgets. Such technique utilizes metadata of apps and Naïve_Bayes calculation for malware identification. The methodology is a static strategy for malware recognition so it can't shield the gadget from malwares which may change their selves dependent on the capacity to decipher, alter and revamping the code belonging to their selves.

The mark based techniques [14, 15] presented in the ninety's, are usually utilized in malware location. The significant shortcoming of such sort of methods is its shortcoming in identifying transformative and concealed malware. Rather than utilizing prior - defined marks for malware identification, information mining and machine learning methods give a powerful method to progressively separate malware designs [16].

One more behaviour - based foot printing technique [17] additionally gives a powerful way to deal with identify self - proliferating malware. For cell phone based versatile processing system, ongoing years have seen an expanding number of increasingly muddled malware assaults, for example, repackaging. An ongoing examination presented in [18] deliberately describes existing Android malware from different perspectives, including the establishment strategies, initiation component just as the idea of conveyed vindictive payloads.

Persuaded by the expanding no. of Apps and the absence of successful malware location devices, few exploration [19] attempt to recognize malware by watching the measurement and additionally powerful conduct and characters of apps. The scholar in [20] presents to utilize consent conduct to recognize novice Android malwares and afterward make uses heuristic sifting for identifying obscure Android malwares.

The work in [21] made separation of the strings in the app, client rating, count of evaluations, size of app, consents and utilized Bayesian_Networks, Decision_Tree, SVM and Random Forest. A sum of 820+ examples were utilized to check and the creators reasoned that they can accomplish a higher precision with reduced false positive ratio.

The work proposed in [22], dissected 796 generous and 175 malevolent apps for the examination. Authorizations utilized out of manifest.xml record and API calls data from the classes.dex document are extricated and along gain of information they chose a lot of 20 applicable API calls. Then looked at the outcomes got by ML calculations, for example, SVM, Naïve_Bayes algorithms, etc.

The work in [23] consolidated the dual kinds of utilized authorization, broadcasting collectors and exercises, byte code pieces, framework calls as highlights and prepared SVM along with training datasets. The authors tried their proposed Malware identification framework along a security analyser for bench - marking where the framework was tried with 7,000 examples. They presume that framework could accomplish overall 99.3% of positive rate along with simply 0.14% bogus alert ratio.

The number of consumers for mobile increasing now a days and there is a possibility of accessing to their data through sensors by third party. The semadroid concept can help the customers in defining sensor usage policies [24].

The use of different devices in the IoT has resulted in various attacks, such as malware.

- To improve the malware detection for Android IoT devices using the combination of different methods like Machine Learning and Blockchain algorithms.

- To improve the security for the Android IoT devices from extensive exploitation of the Android platform in the IoT devices from malwares.
- To improve the run - time detection rate of malwares in Android IoT devices

The Fig. 3 gives the statistical analysis of the advancement of Android malwares worldwide as on May 2019. Till this month, all together count of Android malware recognitions is gathered up to over 10.5 million projects.

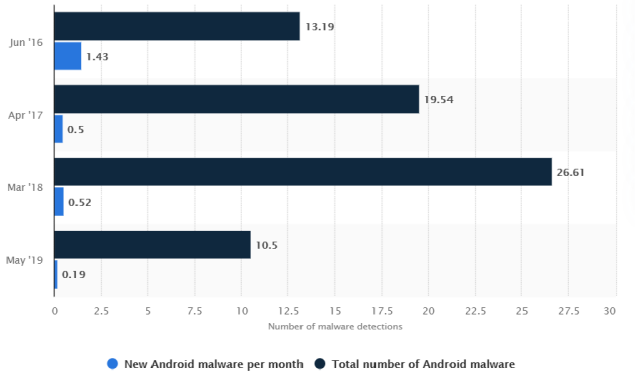

Figure 3: The growth of new Android malware worldwide (in millions) [2]

The Fig. 4 demonstrates that, in second quarter of 2019, the Kaspersky identified 753,550 packages of malicious apps installations, that is 151,624 lesser compared to the preceding quarter.

Throughout current year, observation has made by us, a consistent decrease in the measure of newly created mobile malwares. The reduction is the aftereffect of reduced cybercriminal movement in extending individuals to the much well-known communities. Among all the dangers distinguished in second qurter of 2019, the offer from lions went to possibly spontaneous Risk Tool applications with 41.24%, that is 11 p.p. higher compared to the past quarter. The malevolent articles most every now and again experienced originated out of the Risk Tool.

Android OS. Agent community (33.07% of every single distinguished danger in this interval), RiskTool. Android OS. Wapron (14.41%) and RiskTool. AndroidOS. Smssend (15.68%). In correlations, our work is spurred by a portion of the above procedures and approaches, however with center around creating straightforward and compelling malware recognition methodologies, without depending on complex dynamic execution time investigation and any malware marks which are static and predefined.

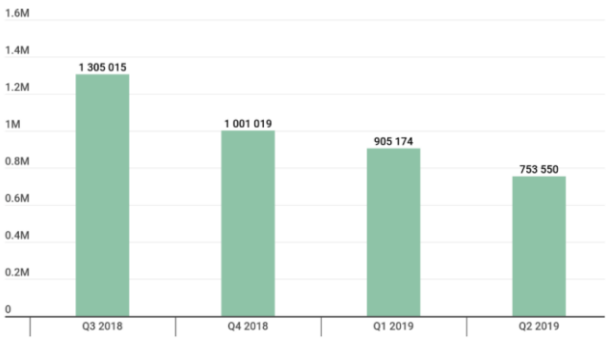

Figure 4: Graphical representation of identified packages of malicious installation [3]

3. COMPARISON OF DIFFERENT METHODS

In correlations, our work is spurred by a portion of the above procedures and approaches, however with center around creating straightforward and compelling malware recognition methodologies, without depending on complex dynamic execution time investigation and any malware marks which are static and predefined. The comparison of various malware detection methods along with their accuracies are presented in table 1.

Table 1: Comparison of various malware detection methods

Sl. No.	Title/work	METHOD	ACCURACY
1	"Classification of Android apps and malware using deep neural networks"	CNN	90%
2	"High Accuracy Android Malware Detection Using Ensemble Learning"	Ensemble ML methods	99%
3	"Feature Selection approach to detect Android malware using Deep Learning"	Deep neural network and PCA	94%
4	"A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting"	Recurrent Neural Network	98.18%
5	"An Android malware detection system based on machine learning	PCA, SVM	95.2%
6	An Android malware detection method based on Android Manifest file"	Naive bayes and pattern mining	88.69%
7	"Android Malware Detection Using Parallel Machine Learning Classifiers"	Parallel ML Approach	97.3%
8	"MLDroid—framework for Android malware detection using machine learning techniques"	Deep learning, MLP, clustering	98.8%

4. CONCLUSIONS

The IoT devices are advancing this world towards a new paradigm with its exciting applications such as sensing, smart healthcare, remote monitoring, smart agriculture, etc. Android platform based IoT devices and applications are working hand to hand to realize IoT dreams. This papers provides study on malware detection for android devices.The paper provides a basic introduction to usage of IOT for android devices with a review on the paper. The paper also compares different work which is carried out earlier.

REFERENCES

1. Hamed Haddad Pajouh, Ali Dehghantanha, Raouf Khayami, Kim - Kwang Raymond

Choo, " A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting, " Future Generation Computer Systems, Vol. 85, p. p. 88 - 96, Aug. **(2018).**

2. AnavBedi, Nitin Pandey, Sunil Kumar Khatri, " Analysis of Detection and Prevention of Malware in Cloud Computing Environment, " 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4 - 6, Feb. **(2019),** p. p. 918 - 921.

3. Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Michael Backes, Patrick McDaniel, " Adversarial Examples for Malware Detection, " European Symposium on Research in Computer Security, Luxembourg, 23 - 27, Sep. **(2019)**, p. p. 62 - 79.

4. W. Peizhuang, " *Pattern Recognition with Fuzzy Objective Function Algorithms, "* Philadelphia, PA, USA: SIAM, 1983.

5. M. S. Yang, " A survey of fuzzy clustering, '' *Math. Comput. Model.*, vol. 18, no. 11, p. p. 1 – 16, 1993.

6. D. M. Witten and R. Tibshirani, "A framework for feature selection in clustering,'' *J. Amer. Stat. Assoc.*, vol. 105, no. 490, p. p. 713 – 726, 2010.

7. X. Wang, Y. Wang, and L. Wang, '' Improving fuzzy *c* - means clustering based on feature - weight learning, " *Pattern Recognit. Lett.*, vol. 25, no. 10, p. p. 1123 – 1132, 2004.

8. Faruki, Parvez, Ammar Bharmal, Vijay Laxmi, Vijay Ganmoor, Manoj Singh Gaur, Mauro Conti, and Muttukrishnan Rajarajan. " Android security: a survey of issues, malware penetration, and defenses. " IEEE communications surveys & tutorials 17, no. 2, (2014), p. p. 998 - 1022.

9. Mahindru, Arvind, and Paramvir Singh. " Dynamic permissions based android malware detection using machine learning techniques. " In Proceedings of the 10th innovations in Software Engineering Conference, (2017), p. p. 202 - 210.

10. Mahindru, Arvind, and A. L. Sangal. " DeepDroid: Feature Selection approach to detect Android malware using Deep Learning. " In 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS), IEEE, (2019), p. p. 16 - 19

11. Vemparala, Swapna, Fabio Di Troia, Visaggio Aaron Corrado, Thomas H. Austin, and Mark Stamo. "Malware detection using dynamic birthmarks. " In Proceedings of the 2016 ACM on International Workshop on Security and Privacy Analytics, (2016), p. p. 41 - 46

12. Baskaran B, Ralescu A. " A study of android malware l detection techniques and machine learning, " In: Phung PH, Shen J, Glass M, editors. Modern Artificial Intelligence and Cognitive Science; 22 - 23 April 2016. Dayton, OH, USA: CEUR; 2016. p. 15 - 23

13. X. Li, J. Liu, Y. Huo, R. Zhang, Y. Yao, " An Android malware detection method based on Android Manifest file, " International Conference on Cloud Computing and Intelligence Systems (CCIS), 2016, p. p. 239 - 243.

14. N. B. Akhuseyinoglu, K. Akhuseyinoglu, " AntiWare: An automated Android malware detection tool based on machine learning approach and official market metadata, " IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2016, p. p. 1 - 7

15. Shabtai, A., et al., " Andromaly" a behavioral malware detection framework for android devices, " J. Intell. Inf. Syst., 2012. 38(1): p. 161 - 190.

16. Arnold, J.O.K.W.C., " Automatic Extraction of Computer Virus Signatures, " In Proceedings of 4th Virus Bulletin International Conference, 1994: p. 178 - 184.

17. M.G. Schultz, E.E., F. Zadok, S.J. Stolfo, " Data mining methods for detection of new malicious executables, " Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001, 2001: p. 38 - 49.

18. Zhu, X.J.X., " vEye: behavioral footprinting for self - propagating worm detection and profiling, " Knowledge and Information Systems, 2009. 18(2): p. 231 - 262.

19. Jiang, Y.Z.X., " Dissecting Android Malware: Characterization and Evolution, " IEEE Symposium on Security and Privacy, 2012: p. p. 95 - 109.

20. Burguera, I., U. Zurutuza, and S. Nadjm - Tehrani, " Crowdroid: behavior - based malware detection system for Android, " in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. 2011, ACM: Chicago, Illinois, USA. p. 15 - 26.

21. Mr. Dharmesh Dhabliya, Mr. Rahul Sharma. (2012). " Efficient Cluster Formation

Protocol in WSN, ” International Journal of New Practices in Management and Engineering, 1(03), 08 - 17.

22. Yajin Zhou, Z.W., Wu Zhou, Xuxian Jiang, Hey, “ You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets, ” network and distributed system security symposium, 2012.

23. B. Sanz, I. Santos, C. Laorden, X. Ugarte - Pedrero, and P.G. Bringas. “ On the automatic ategorisation of android applications, ” In Consumer Communications and Networking Conference (CCNC), 2012 IEEE, pages 149 – 153, Jan 2012.

24. Zhi Xu and Sencun Zhu. (2015) “ SemaDroid: A Privacy - Aware Sensor Management Framework for Smartphones, ” In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. San Antonio, Texas, USA, 61 - 72.

25. R. Nix and J. Zhang, " Classification of Android apps and malware using deep neural networks, ” *Proc. Int. Joint Conf. Neural Netw.*, p. p. 1871 - 1878, May 2017.

26. S. Y. Yerima, S. Sezer and I. Muttik, " High accuracy android malware detection using ensemble learning,” *IET Inf. Secur.*, vol. 9, no. 6, p. p. 313 - 320, Nov. 2015.

27. Long Wen, Haiyang Yu, “ An Android malware detection system based on machine learning, ” AIP Conference Proceedings 1864, 020136 (2017)

28. Suleiman Y. Yerima, Sakir Sezer, Igor Muttik, “ Android Malware Detection Using Parallel Machine Learning Classifiers ” 8 th International Conference on Next Generation Mobile Applications, Services and Technologies, (NGMAST 2014), 10 - 14 Sept., 2014

Corresponding Author

Baviskar Pallavi Vasudev*

Phd Student. Kalinga University, Raipur