Predicting Fraud Apps using Hybrid Learning Approach

K.Aishwarya[1] , C.Selvi[2]

[1] Student Scholar, Department Of CSE, Velalar College of Engineering and Technology, Erode, TamilNadu-638012, India.

[2] Associate Professor, Department Of CSE, Velalar College of Engineering and Technology, Erode, TamilNadu-638012, India.

Abstract

Mobile phone has become the target for risky and snoopy applications. The android's current risk communication technique depends on users to identify the permissions that an app is requesting. But the users are unaware of permissions as it requires some technical knowledge. Therefore, android's protection against malicious application is risk communication method where any user who wishes to install an app will be warned about permissions, the application would call for and then the user has to take the proper decision. In Google play, the users frequently download and use several applications from various unknown vendors. Therefore, the protection against malware applications should depend on decisions made by users. The main part of protection against malware on mobile devices is to alert the users about malware and permit them to take decisions about whether to choose and install specific apps. Compute risk score that users can apply while choosing applications whether they want to use that app or not.

Keywords — *Android Devices, Security Fraud detection, Reviews.*

I. INTRODUCTION

Mobile devices are widely used due to its popularity and functionality. Smart phones have become trendy for private and business use in recent years. All details are stored on the devices, which include contact lists, email messages, passwords, private information and access to those information that are stored locally and in the cloud. With the arrival of smart phones, users have their private information with them on their phones. This information ranges from location of the phone and also their bank particulars. While attacks on mobile devices have mainly focused on stealing users personal data contained on the devices. Possible access to confidential information by unknown person puts users at risk. As the Android platform has developed to take one of the major shares of the smart-phone market, it turns out to be the prime target for criminals who are in search of the private data about users. Simultaneously, the security of the platform has come under scrutiny from security professionals. Malicious software is a problem for all software platforms, and Android platform is no exception. Since the initial malicious application was discovered in 2010, now the number of malicious applications has been constantly rising. Therefore, to execute malicious behavior, attackers have to trick users to install a malicious app since no other way is possible for intrusion in Android. Moreover, a common user does not have proper technical knowledge about the Android permissions and their impacts. An Android malware e.g., spyware, Trojan, Adware, can trick the users by introducing itself as a useful app and stole their private or business information. There exist some assessments in order to get better security mechanism. With improved and intuitive titles for permissions, classification of permissions based on their effects, reducing the number by integrating related ones, utilizing user reviews about apps, using visual security indicators for risky apps are few work for enhancing android security mechanism.

II. LITERATURE SURVEY

The android's basic defense mechanism against malicious applications is a risk communication system which cautions the client about the permissions before the client introduces an application [2]. This method was unsuccessful as it shows the risk information of every application in a "stand alone" manner and in a way that requires focused learning and a lot of time to distil important data [3]. Check the required properties of risk signals for Android applications with the end goal to generate another metric that clients can utilize while choosing applications [4]. Show a wide range of techniques to formulate risk scores that focus on heuristics and also principled machine learning systems. Trial comes on directed utilizing certifiable information sets that show that these techniques can identify malware as dangerous, are simple to figure out, and easy to exploit [5]. There are distinct and huge numbers of applications on the Play store where a few of them look similar. Moreover various applications are duplicate and also fraud application which contains malware. They may get information from the android and may damage the android device anytime. Such applications also have client ratings and review which figures out the benign and fraud application. In android application, it has rundown of uses from a variety of classes for which it is necessary to identify whether it is fake or not [6]. Mobile vide contact to individual person and fragile data devices are getting universal, and they are telephone records, call lists, geolocation, and SMS messages, making their safety a very important test [7]. In play store users download and utilize numerous applications. The protection against malware applications depends on users [8]. An important part of malware protection on mobile devices is to reveal about the risk of installing the application to clients and to allow the user to take decisions about whether to select and install the applications [9].

III. PROPOSED SYSTEM

The proposed framework categorizes the applications in Google play as benign or fraud application using Naïve Bayes classifier. The proposed solution can be used by both mobile users to make better decision and android markets to filter suspicious applications. In this method malware detection in Google play mainly focuses on similarity matching and behavior profiling to detect suspicious application. This proposed method contains four modules. The first module is the Co-Review Graph module which identifies apps reviewed in a contiguous time by groups of users. The second module called as Review Feedback module identifies feedback left by genuine reviewers. The third module called as Inter Review Relation module consider the relations between reviews and install counts as well as between average rating and install counts. The last module called Jekyll-Hyde is used to identify the permission requested for applications and it also involves in monitoring the permission until the user removes the application. It incorporates Naïve Bayes classification algorithm and the classifier was trained using gold standard data sets.

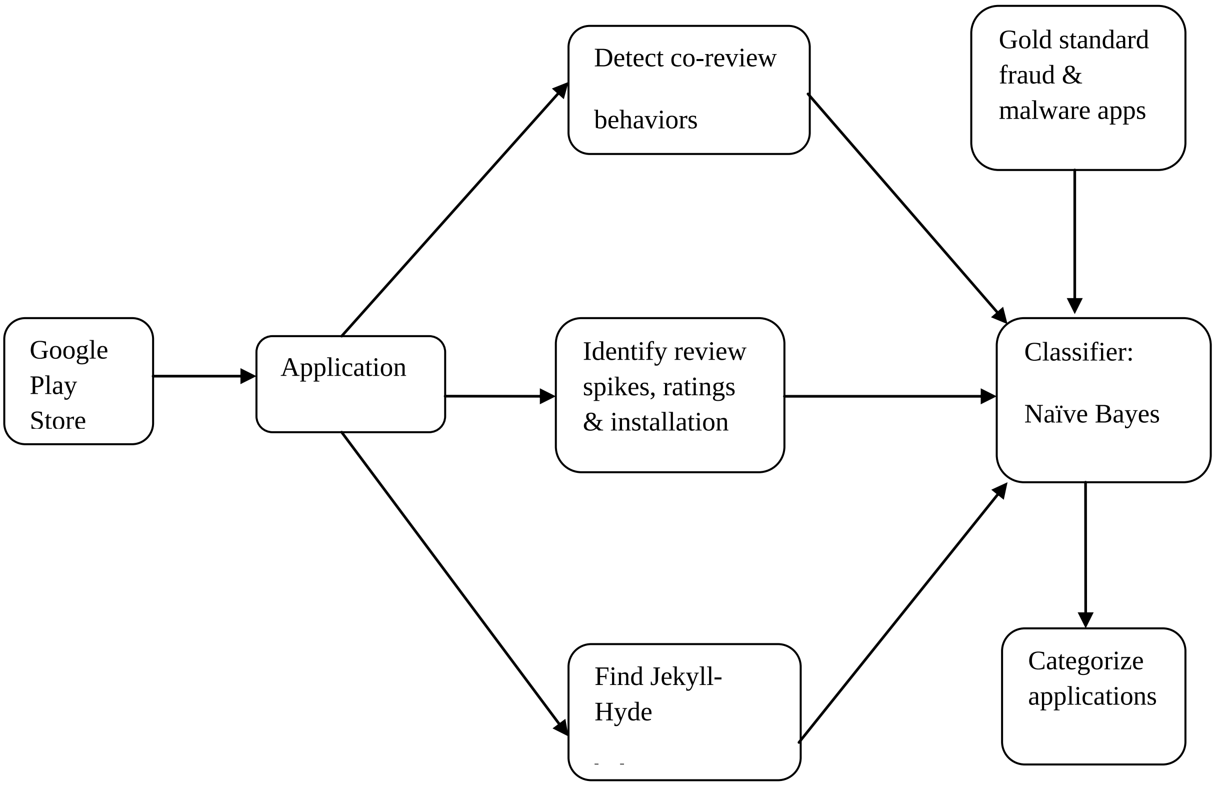

fig 1 : System Architecture

A. *Naive Bayes Model*

Naive Bayes is the technique which is used for constructing classifiers: it assigns class labels to problem instances, which was indicated as vectors of feature values, where the class labels are derived from some finite set. It is not just a single algorithm for training such classifiers, but a family of algorithms and they are based on a common principle: all Naive Bayes classifiers imagine that the value of a particular feature does not depend on the value of any other feature for any given class variable.

B. Naive Bayes Classification Algorithm

The Naive Bayes is a classification algorithm and it is based on Bayes theorem. The word naive from Naive Bayes comes from the fact that the algorithm takes Bayesian techniques and it ignores dependencies that may exist. This algorithm is less computationally intense than other algorithms and therefore it is helpful for generating mining models to find out relationships between input columns and predictable columns. It trains the classifier in order to identify fraud apps. They are trained using gold standard datasets. Thus Naïve Bayes is effective in predicting fraud application in Google play as it requires less training data.

IV. CONCLUSION

Most of the android users are unaware about the permissions requested for application. Thus, mobile devices become target for fraudsters. This made fraudster to break the security of mobile devices and steal user's confidential information. Sometimes the applications get updated. Whenever updated versions of applications are installed, it is difficult for users to identify whether the updated version contains malware or not. The existing techniques are ineffective in identifying malware as they consider only one factor for predicting malware i.e. reviews or permissions. Therefore, this work mainly focused on user reviews, ratings and permission of each android app. It helps to filter applications and recognize malware and fraud application. The user reviews and ratings are also evaluated to recognize fraud reviews. Reviews are evaluated to identify genuine and fraud reviews. Thus, it helps to figure out benign and fraud apps. It adapts classification techniques for classifying applications thus improving the security of android devices.

ACKNOWLEDGEMENT

I would like to sincerely express thanks to my guide C.Selvi for her appreciable support, continuous encouragement and for her valuable suggestions. I am grateful for all the suggestions and hints provided by her. It was great moment to work with my guide.

REFERENCES

[1] Mahmudur Rahman, Mizanur Rahman, Bogdan Carbunar, and Duen Horng Chau, "Search Rank Fraud and Malware Detection in Google Play, IEEE Transactions On Knowledge And Data Engineering,Vol. 29,No.6 June 2017.

[2] M.Nauman, S. Khan, and X. Zhang, "Apex: Extending Android Permission Model and Enforcement with User-Defined Runtime Constraints," Proc. Fifth ACM Symp. Information, Computer and Comm. Security, pp. 328-332, 2010.

[3] R.Surendiran,Dr.K.Alagarsamy,"An Extensive Survey on Mobile Security and Issues",International Journal of Computer & Organization Trends(IJCOT) – Volume2 Issue1 2012,ISSN: 2249 - 2593, Page 39 - 46.

[4] K.L.R.S.Himaja, Mrs.T. Sri Lakshmi,"Providing Security to User Data using OTP and Image CAPTCHA",International Journal of Computer & Organization Trends (IJCOT),Volume - 6 Issue - 6 2016.

[5] R.Surendiran,Dr.K.Alagarsamy,"A Novel Tree Based Security Approach for Smart Phones",International Journal of Computer Trends and Technology(IJCTT)-Volume 3 Issue 6 – 2012,ISSN: 2231 - 2803, Page 787 - 792.

[6] Christopher S. Gates, Ninghui Li, Senior Member, IEEE, Hao Peng, Bhaskar Sarma, Yuan Qi, Rahul Potharaju, Cristina NitaRotaru, Member, IEEE Computer Society, and Ian Molloy "Generating Summary Risk Scores for Mobile Applications," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 3, MAY-JUNE 2014.

[7] A.P.Felt, K. Greenwood, and D. Wagner, "The Effectiveness of Application Permissions," Proc. Second USENIX Conf. Web Application Development, (WebApps '11), 2011.

[8] R.Surendiran,Dr.K.Alagarsamy,"Privacy Conserved Access Control Enforcement in MCC Network with Multilayer Encryption",International Journal of Engineering Trends and Technology (IJETT),Volume4 Issue5 2013,2231-5381, Page 2217 - 2224.

[9] Dr.V.P.Eswaramurthy , M.Arthi,"A Survey on Image Mining Techniques"International Journal of Computer & Organization Trends (IJCOT),Volume - 4 Issue - 5 2014.

[10] Christopher S. Gates, Jing Chen, Ninghui Li, Senior Member, IEEE, and Robert W. Proctor, "Effective Risk Communication for Android Apps," IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 3, 2014.

[11] T.Vidas, N. Christin, and L.F. Cranor, "Curbing Android Permission Creep," Proc. Workshop Web 2.0 Security and Privacy, vol. 2, 2011.

[12] H.R.Divakar, Dr.B.R.Prakash,"Classics of Deep Learning Approach for Human Behaviour Ontology: A Survey",International Journal of Computer Trends and Technology (IJCTT),Volume-51 Number-1,2017.

[13] S.Gavaskar,R.Surendiran,Dr.E.Ramaraj,"Three Counter Defense Mechanism for TCP SYN Flooding Attacks",International Journal of Computer Applications,Volume 6– No.6, September 2010,ISSN: 0975 – 8887, Page 12 - 15.

[14] B.P.Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy, "Android Permissions: A Perspective Combining Risks and Benefits," Proc. 17th ACM Symp. Access Control Models and Technologies (SACMAT '12), 2012.

[15] M.Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, "RiskRanker: Scalable and Accurate Zero-Day Android Malware Detection," Proc. 10th Int'l Conf. Mobile Systems, Applications, and Services, (MobiSys '12), pp. 281-294, 2012.

[16] SY Yerima, S Sezer, G McWilliams - IET Information Security, 2014 - ieeexplore.ieee.org "Analysis of Bayesian classificationbased approaches for Android malware detection."