ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

Confidentiality Preserving Using Crowdsourcing for Android Users

Narendra Eswar G[1], Yashwant Rahul C.N[2], Bhaskar N[3]

B.Tech, Department of Information Technology, K.C.G. College of Technology, Chennai, India

Assistant Professor, Department of Information Technology, K.C.G. College of Technology, Chennai, India

ABSTRACT: In the present Android system, users have to decide whether an app is safe to use or not. Users are not precisely skilled or they don't care their privacy consequences to make benign decisions. To guide the theoretically unqualified crowd, this project proposes an Android application to find whether a third-party application is safe to use or not. In this application, the user has to register and then login ,the third party application must be selected for installation and then it has two modes: Probation Mode and Trusted Mode. Application runs only in the probation mode. The permissions for the third-party application will be given by the user and then it will be stored in the database. Then by that, the expert users are identified using crowdsourcing algorithms. The permissions given by the user are been analyzed based on the expert rankings and rating whether to accept the third-party application for installation or reject it.

KEYWORDS: Crowdsourcing, Mobile Application, Privacy Permissions.

I. INTRODUCTION

The android is a mobile working system which is established by Google, based on a altered version of the Linux kernel and with open foundation software and designed mainly for touch-screen mobile devices such as Smartphone and tablets. Google has further established Android for televisions, Android for cars, and Android for wrist watches, each with a expert user interface. Android are also been used on various games, digital cameras, personal computers and other electronics. The operating system has subsequently gone through many major proclamations, with the current version presence 8.1. Android has been the blockbusting OS worldwide on Smartphone. Google Play store features over 3.5 million applications. The android default handler interface handles, like touch inputs that approximates to real-time actions, like swiping on both the sides, tapping, zooming in, and zooming out on objects, along with a virtual keyboard. The response to user input is designed to be immediate and provides a unsolidified touch interface, often using the vibration capabilities of the device to provide hepatic to the user. MOBILE apps have brought tremendous impact to businesses, social, and lifestyle in recent years. Various app markets offer a wide range of apps from entertainment, business, health care and social life. Android app markets, which share the largest user base, have gained a tremendous momentum since its first launch. According to the report by Android Google Play Store, the number of apps in the store has reached 2.2 million surpassing its major competitor Apple App Store. The rise of Android phones brought the propagation of Android apps, resulting in an ever-growing application ecosystem. As users rely more on mobile devices and apps, the privacy and security concerns become important. third-party apps not only steal private details, such as contact list, text messages, online accounts, and location from their users, but also cause financial loss to users by making secretive premium-rate phone calls and text messages. At the same time, the rapid growth in the number of apps makes it not practical for app market places, such as Google App Store, to systematically verify if an app is malicious or not. As a result, mobile users are left to decide whether an app is safe to use or not. More specifically, beginning in Android (API level 23), user grants permissions to apps while the apps are running. Users can also manually revoke permissions from any app, even the ones designed for old versions of Android. Unauthorized communications among apps are prohibited. However, such permission control mechanism has been proven to be unsuccessful in protecting users from malicious apps. A study shows that more than 70% of smartphone apps request to collect data unrelated to the main function of the app. Among the 1.4 million apps in Google Play, a significant

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

percentage of them have permissions going beyond the apps' future use. The situation is even not as good as in the third-party markets which are also available to Android users. In addition, such study shows that only a very small portion (3%) of users pay attention and makes correct responses to requests for resource permission at installation, since they tend to rush through to get to use the application. The current Android permission warnings do not help users to make correct decisions. the reasons for the ineffectiveness of the current permission control system include: (1) inexperienced users do not realize resource requests are irrelevant and could compromise their privacy, (2) users have the urge to use the app and may be have to give up their privacy in order to use the app. To address this problem, we propose an application to assist mobile users in controlling their resource usage and privacy through crowdsourcing. Crowdsourcing has been widely applied to address problems ranging from basic to composite in a variety of disciplines, including information systems development, marketing and operationalization. As an application of crowdsourcing, it can be used in the recommendation based systems. Crowdsourcing acts as a spread human intelligence mediator in a recommendation-based system. Opinions are asked and are aggregated to make a recommendation based on a decision problem. The crowdsourcer will obtain and use to their advantage that which the user has brought to the scheme, whose form will depend on the type of activity undertaken. Specifically, our application allows users to install untrusted apps under a "probation"mode, while the trusted ones are installed in normal "trusted"mode. In probation mode, users make real-time process granting decisions when the applications are running. The application facilitates a user-help-user environment, where expert users are identified and their decisions are recommended to inexperienced users

II. RELATED WORK

Crowdsourcing has been widely applied to address problems ranging from basic to complex in a variety of disciplines, including information systems development, marketing and operationalization. As an application of crowdsourcing, it can be used in the recommendation based systems. Crowdsourcing acts as a distributed human intelligence agent in a recommendation-based system in which participants? (human individuals) opinions (solutions) are asked and later aggregated to make a recommendation on a decision problem. Exploring user perceptions of privacy on smartphones using crowdsourcing has already been investigated. Agarwal and Hall propose PMP which collects users' privacy protection decisions and analyses them to recommend them to other iOS users. However, their recommendations are based on simple majority voting which results in high false recommendation rates. Investigated people's privacy preferences by capturing apps logs and analyzing them to identify a small number of profiles that simplify decision makings for mobile users. Profiles were mined from logs by using SVM techniques. However, they do not include users' expertise in their study and this might cause false recommendation. Investigated the feasibility of identifying a small set of privacy profiles to help users manage their privacy profiles. Instead of relying on smartphone users' decisions on permission requests, they identified the privacy profiles using Androguard, a static code analysis tool. They analyzed the purpose for which an app requests permission and identified the permissions that satisfy the least privilege policy. Thus, they can find a set of necessary permissions for apps.In the proposed PriWe in which they crowd source users' decisions on permission requests and identify users' expectations. In their work, they focus on finding users with similar responses to permission requests. After finding similar users and applying a recommendation algorithm they identify some privacy profiles and recommend them to those who have similar strategy for responding to permission requests. This paper proposes a crowdsourcing solution to find a minimal set of permissions that will preserve the usability of the app for diverse users. Their approach has a few shortcomings. Repackaging apps for all possible permission combinations is not practical. Also their inability to differentiate between inexperienced and malicious users makes their recommendations of limited quality. It propose a system to allow users to share their permission reviews with each other. Users leave comments on permissions and the system ranks reviews and recommends top quality reviews to users. The system proposes, an analysis technique that analyzes app behavior while taking into account the context and semantics of the app. Our system uses a two-phase crowd analysis approach, in which crowd workers are asked whether it makes sense for the application to use its requested resources and tasks. App Ops, a feature in Android v4.3, allows users to selectively disable permissions for apps on their phones. However, Google removed this feature in their next update, reporting that it was experimental and could cause apps to behave in unexpected ways. The common feature of those approaches is that they do not consider users' expertise in privacy profiling or permission recommendations. In contrast, considering the fact that most users are inexperienced, we

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

proposed an expertise ranking algorithm to evaluate the expertise level of users for higher quality recommendations. In previous work they proposed to utilize expert users' decisions to help inexperienced users on Android permission control. In this paper, we developed an expert seeking and a decision recommendation algorithm based on iterative algorithm. There have been several applications of crowdsourcing in recommendation-based systems in contexts other than smartphone privacy. For example, using crowdsourcing recommendation-based system to learn personal preferences of customers in e-commerce applications. Crowdsourcing recommendation-based systems are also being used to improve the performance of workers at work environments. The role of the recommendation-based system is to collect workers' profiles, explicit worker feedback, user-task interaction and task details and process them in order to make a recommendation on which tasks should be assigned to which worker. Designing a recommendation-based system that achieves high level of accuracy would be a great opportunity for solving issues through a distributed human intelligence system.

III. METHODOLOGY

Our proposed system has 3 modules Installation mode, Access permissions, Access request. the user has to register and then login. Firstly, the installation mode has 2 modes probation and trusted mode. Before installing an app, get the mode from the user either probation mode or trusted mode. If the user selects the trusted mode, then the application will be installed with all requested permissions granted. The application will run only when the user selects the probation mode. On the other hand, if the user selects the probation mode, then the application will be added to a list of monitored apps on the mobile phone. After the Installation mode the user have to give permissions. The permissions for the application will be given by the user and then it will be stored in the database. The expert users are identified using crowdsourcing algorithms. The algorithms used are iterative algorithm and TOP-K-E algorithm to get the best expert users. In this iterative algorithm is used to differentiate expert from non-expert users by using this algorithm only find the experts. To increase the efficiency of finding the best experts the algorithm used is TOP-K-E where the best experts are selected to check the application's confidentiality. Then recommendation algorithm is used to give suggestions based on the experts rating and gives the solution whether to accept or reject the application to be installed. The access request is analyzed based on the expert rating whether to accept the third party application for installation or reject it. Confidentiality of third party application is given to the end user using the above algorithms through an application.

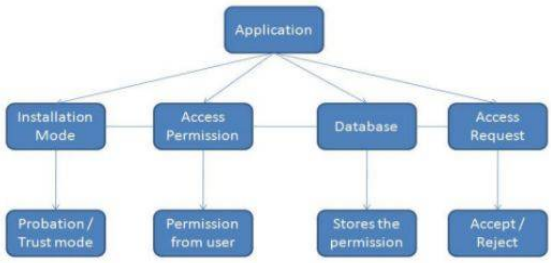

FIGURE NO.1 METHODOLOGY FOR CONFIDENTIALITY PRESERVING USING CROWDSOURCING FOR ANDROID USERS.

ALGORITHM

TOP-K-E ALGORITHM

1: Compute top experts
2: Notations:
3: F(u): the current rating of all users
4: F^(u): the last round rating of all users
5: s: the seed expert
6: Un: the nth user

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

7: EU: the set of rated users
8: QU: the queue of users to be rated
9: set F(s) = 1 and F(U) = 0.5
10: while (Distance(F(u), F^(U)) >0) do
11: EU ← s
12: QU ← f indNeighbors(s)
13: F^(u) ← F(u)
14: while (u ←remove(QU) is not null) do
15: R(u) ←computeRating(u)
16: EU ← EU ∪ u
17: X = f indNeighborsNot I nEU or QU
18: push(X, QU)
19: end while
20: end while

The current rating of all users is denoted as f(u). the last round rating of all users is denoted as f^ (u). The seed experts are denoted as se. un is the nth user. eu is denoted as set of rated users. qu is the number of users to be rated in the queue. Gather the entire user rating available in the database which are given by the users. Rating of all the users can be varied for each round of iteration. Iteration can be performed once when the user is connected to seed user directly or indirectly. if any user already rated during previous iteration make them as seed experts in this iteration then the number of new users must be found. Also need to check number of user who is waiting to be rated (qu). Push the unvisited user to the queue. The iteration will check the number of user rated and the last round rating of all the user if the difference between two rounds of rating is sufficient close then the iteration will stop. if new user are in the queue then check common between the previous rating and the user provided information to say they are seed users or not.

RECOMMENDATION ALGORITHM

1: Notations :
2: Rs(u),Cr(u) :the rating score and rating confidence of user u
3: f(u) :the response to permission request from user u
4: te, tc :the minimum rating score and rating confidence to be considered as an expert user
5: td :the recommendation threshold
6: Y,N :the cumulative ballots for yes or no decision
7: D0 :the initial ballot count for both decisions
8: Y = N = D0
9: for each user u who responded to the request do
10: if Rs(u) >te and Cr(u) >tc then
11: if f(u) = 1 then
12: Y+ = Rs(u)
13: else
14: N+ = Rs(u)
15: end if
16: end if
17: end for
18: if Y/Y+N > td then
19: Accept the request with confidence Y/Y+N - td
20: else if Y/Y+N < 1 − td then
21: Recommend to reject the request with confidence 1 − Y/Y+N − td
22: else
23: No recommendation
24: end if

After rating the users, recommendations are done. rs(u),cr(u) are the rating score and rating confidence of user u. f(u) is the response to permission request from user u. te, tc are the minimum rating score and rating confidence to be

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

considered as an expert user. td is the recommendation threshold . y is the user who accept the application, n is the user who reject the application . d0 is the initial ballot count for both decisions. y = n = d0. for each user u who responded to the request, if the rating score is greater than the minimum rating score & rating confidence is greater than the minimum rating confidence then if the user accepts the application ,y gets incremented. else if the user rejects the application ,n gets incremented. if y/y+n is greater than recommendation threshold then recommend the user to accept the request with confidence. else if y/y+n is less than 1 − recommendation threshold then recommend the user to reject the request with confidence.

IV. CONCLUSION

In this paper we present an application, permission control and recommendation system which serves the goal of helping users perform low-risk resource accessing control on untrusted apps to protect their privacy and potentially improve efficiency of resource usages. We propose a framework that allows users to install apps in either trusted mode or probation mode. In the probation mode, users are prompted with resource accessing requests and make decisions on whether to grant the permissions or not. In order to do so, application uses crowdsourcing techniques to search for expert users using a iterative algorithm. Our evaluation results demonstrate that our application can effectively locate expert users in the system through a small set of seed experts. The recommending algorithm achieves high accuracy and good coverage when parameters are carefully selected. We implemented our application on Android phones and demonstrate that the system is feasible and effective through real users experiments.

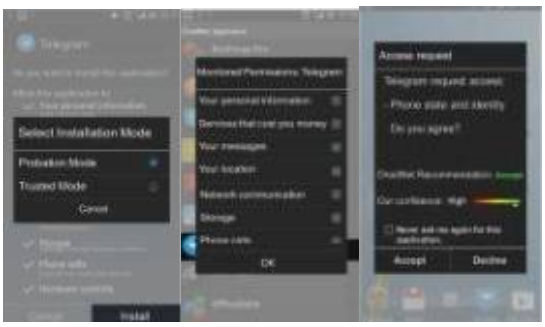

Figure No.2 Output of the Implementation

REFERENCES

1. "ANDROID USER PRIVACY PRESERVING THROUGH CROWDSOURCING" BahmanRashidi , Student Member, IEEE, Carol Fung, Anh Nguyen, Tam Vu, and Elisa Bertino, Fellow, IEEE Transactions on Information Forensics And Security Vol. 13,No. 3, March 2018 .
2. "REAL-TIME RECOMMENDATION ALGORITHM FOR CROWDSOURCING SYSTEMS" MejdlSafrana ,DunrenChe Computer Science Department, Southern Illinois University, Carbondale, IL, USA Computer Science Department, King Saud University, Riyadh, Saudi Arabia Applied Computing and Informatics (2017).
3. "PriWe: RECOMMENDATION FOR PRIVACY SETTINGS OF MOBILE APPS BASED ON CROWDSOURCED USERS EXPECTATIONS" Rui Liu, Jiannong Cao, Lei Yang Department of Computing The Hong Kong Polytechnic University Hong Kong Kehuan Zhang Department of Information Engineering The Chinese University of Hong Kong Hong Kong 2015 IEEE International Conference on Mobile.
4. WHAT IS THE PRICE OF FREE. ACCESSED: OCT. 1, 2017. [ONLINE]. AVAILABLE: http://www.cam.ac.uk/ research/news/what-is-the-price-of-free.
5. APPS BY DOWNLOADS: DOWNLOAD DISTRIBUTION OF ANDROID APPS. Accessed: Aug. 2017. [Online]. Available: https://www.appbrain.com/stats/androidapp-downloads
6. DOWNLOAD STATISTICS: DISTRIBUTION OF DOWNLOADS IN THE ANDROID MARKET. Accessed: Aug. 2017. [Online]. Available: http://www.androlib.com/ appstatsdownloads.aspx
7. [4] GARTNER: 1.1 BILLION ANDROID SMARTPHONES, TABLETS EXPECTED TO SHIP IN 2014. Accessed: May 2015. [Online]. Available: http://www.reuters.com/ article/us-mobile-devices-gartner/more-than-1-billion-android-devicestoship-in-2014-gartner-idUSBREA060E220140107

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

8. Y. AGARWAL AND M. HALL, "PROTECTMYPRIVACY: DETECTING AND MITIGATING PRIVACY LEAKS ON IOS DEVICES USING CROWDSOURCING," in Proc. 11th Annu. Int. Conf. Mobile Syst., Appl., Services (MobiSys), New York, NY, USA, 2013, pp. 97–110.
9. E. ALDHAHRI, V. SHANDILYA, AND S. SHIVA, "TOWARDS AN EFFECTIVE CROWDSOURCING RECOMMENDATION SYSTEM: A SURVEY OF THE STATE-OF-THEART," in Proc. IEEE Symp. Service-Oriented Syst. Eng., Mar. 2015, pp. 372–377.
10. R. AMADEO. APP OPS: ANDROID 4.3'S HIDDEN APP PERMISSION MANAGER, CONTROL PERMISSIONS FOR INDIVIDUAL APPS! [Online]. Available: http:// www.androidpolice.com/2013/07/25/app-ops-android-4-3s-hidden-apppermission-manager-control-permissions-for-individual-apps/
11. AMBATI, S. VOGEL, AND J. CARBONELL, "TOWARDS TASK RECOMMENDATION IN MICRO-TASK MARKETS," in Proc. 11th AAAI Conf. Human Comput. (AAAIWS), 2011, pp. 80–83.
12. S. AMINI, "ANALYZING MOBILE APP PRIVACY USING COMPUTATION AND CROWDSOURCING," Ph.D. dissertation, Dept. Elect. Comput. Eng., Carnegie Mellon Univ., Pittsburgh, PA, USA, 2014.
13. M. BACKES, S. BUGIEL, C. HAMMER, O. SCHRANZ, AND P. VON STYP-REKOWSKY, "BOXIFY: FULL-flEDGED APP SANDBOXING FOR STOCK ANDROID," in Proc. 24th USENIX Secur. Symp. (USENIX Security),
14. P. G. KELLEY, S. CONSOLVO, L. F. CRANOR, J. JUNG, N. SADEH, AND D. WETHERALL, "A CONUNDRUM OF PERMISSIONS: INSTALLING APPLICATIONS ON AN ANDROID SMARTPHONE," in Financial Cryptography and Data Security. Springer, 2012, pp. 68–79.
15. P. FELT, E. HA, S. EGELMAN, A. HANEY, E. CHIN, AND D. WAGNER, "ANDROID PERMISSIONS: USER ATTENTION, COMPREHENSION, AND BEHAVIOR," in Proceedings of the Eighth Symposium on Usable Privacy and Security. ACM, 2012, p. 3.
16. Q. DO, B. MARTINI, AND K.-K. R. CHOO, "ENHANCING USER PRIVACY ON ANDROID MOBILE DEVICES VIA PERMISSIONS REMOVAL," in System Sciences (HICSS), 2014 47th Hawaii International Conference on. IEEE, 2014, pp. 5070–5079.
17. J. LIN, S. AMINI, J. I. HONG, N. SADEH, J. LINDQVIST, AND J. ZHANG, "EXPECTATION AND PURPOSE: UNDERSTANDING USERS' MENTAL MODELS OF MOBILE APP PRIVACY THROUGH CROWDSOURCING," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing. ACM, 2012, pp. 501–510.