

PRADROID: PRIVACY RISK ASSESSMENT FOR ANDROID APPLICATIONS

Submitted in partial fulfilment of the requirements
for the award of
Bachelor of Engineering degree in Computer Science and
Engineering By

Name : A.Siva
Reg No : 38110535



**DEPARTMENT OF COMPUTER SCIENCE AND
ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND
TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC

**JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI - 600 119**

MARCH - 2022



SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of "SIVA.A (38110535)" under my supervision from December 2021 to March 2022.

DR.MERCY PAUL SELVAN M.E., PH.D.
Internal Guide

DR. L. LAKSHMANAN M.E., PH.D.
Head of the Department

Submitted for Viva-voce Examination held on_____

Internal Examiner

External Examiner

DECLARATION

We **Siva A**(38110645) hereby declare that the Project Report entitled “**Privacy Risk Assessment for Android Application**” done by us under the guidance of **DR. Mercy Paul Selvan M.E.,PHD** (internal) is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering / Technology degree in **Computer Science and Engineering**.

DATE:

PLACE:

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to the **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph.D, Dean**, School of Computing **Dr. L. Lakshmanan M.E., Ph.D. ,** and **Dr.S.Vigneshwari M.E., Ph.D. Heads** of the Department of Computer Science and Engineering for providing me with the necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.Mercy Paul Selvan M.E.,Ph.d.** for her valuable guidance, suggestions and constant encouragement that paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering who** were helpful in many ways for the completion of the project.

ABSTRACT

- The interface allows the user to search for an arbitrary application on the Play Store; the permissions list and the privacy policy are then automatically retrieved, whenever possible.
- The user has then the ability of selecting a specific permission, and a list of relevant sentences are extracted by the privacy policy and presented to them, along with an accurate description of the permission itself.
- Such an interface allows the user to quickly evaluate the privacy-related risks of an Android application, by highlighting the relevant sections of the privacy policy and by providing useful information about sensible permissions.
- We presented a novel approach to the analysis of privacy policies in the context of Android applications.
- The tool we implemented greatly eases the process of understanding the privacy implications of installing third party apps and it has already been proven able to highlight worrisome instances of applications.
- The tool is developed with expandability in mind, and further developments in the approach can easily be integrated in order to increase the reliability and effectiveness.
- In addition, if your app handles personal or sensitive user data, please also refer to the additional requirements in the "Personal and Sensitive Information" section below.
- These Google Play requirements are in addition to any requirements prescribed by applicable privacy or data protection laws.

Contents

<u>1 INTRODUCTION</u>	1
<u>2 LITERATURE REVIEW</u>	3
<u>3 METHODOLOGY</u>	5
<u>4 EXISTING SYSTEM</u>	6
<u>5 PROPOSED SYSTEM</u>	6
<u>6 SYSTEM ARCHITECTURE</u>	7
<u>7 SYSTEM REQUIREMENTS</u>	8
<u>8 MODULES</u>	9
<u>9 CONCLUSION</u>	11
<u>10 REFERENCES</u>	11

INTRODUCTION

Mobile devices of various operating systems have exhibited a steep increase in the past decade, thus leading to an increase in the number and variety of applications that run on mobile devices. Smartphones are recently used either in a complementary manner to a desktop computer or even to replace it. A closer look at the purpose of using mobile phones reveal that they are mostly used for web browsing, social networking, and online banking. In addition, they are used for mobile-specific functions such as SMS messaging, real-time broadcasting of location, and ubiquitous access. As the capabilities in mobile phone functionality increase (e.g., applications for personal health), mobile phones become more and more attractive for a wider population. Market data surveys reveal that the number of smartphone sales worldwide reached 208 million in 2012.

This was a 38.3% increase compared to the sales in 2011. The development of smartphones and mobile applications has resulted in a major change in people's way of doing tasks in various aspects of daily life, such as making business and conducting social communication. Mobile phone applications exhibit a rich variety not only in common daily life activities but also for users with more specific needs. From games to multimedia applications, navigation systems, and health-related applications, recently available mobile application markets, such as Google's Play Market, Apple's App Store, or Microsoft's Windows Store offer a wide variety of applications to users with different needs.

The major application markets have been growing steadily both in terms of the applications offered to the users and the downloads performed by the users. The fast increase in the popularity of smartphones has led to an increase in their potential as a target for malicious activities.

This is mainly because users provide access for various types of private information by means of mobile applications. As a result, some applications in the market have been identified as performing malicious activities. The spread of malicious software is also influenced by the policy of the market providers. For instance, Apple's App Store recently applies a policy that is subject to strict registration and company-issued digital certification before the release of any application, thus providing a security check for the applications listed in their application platform regularly. Others, such as Google's Play Market, introduce more freedom to developers in uploading their own software to the market. The applications are then removed from the market in case of reported malicious activity. In particular, the Android operating system (in its recent form) allows removal of the malicious application from the device remotely. A similar mechanism of removal is also employed by Apple's App Store. The policy of post-detection removal of malicious software brings the need for early detection of malware applications.

LITERATURE REVIEW

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then the next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system. The major part of the project development sector considers and fully survey all the required needs for developing the project. For every project Literature survey is the most important sector in software development process. Before developing the tools and the associated designing it is necessary to determine and survey the time factor, resource requirement, man power, economy, and company strength. Once these things are satisfied and fully surveyed, then the next step is to determine about the software specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations.

Analysis of Bayesian classification-based approaches for Android malware detection

Mobile malware has been growing in scale and complexity spurred by the unabated uptake of smartphones worldwide. Android is fast becoming the most popular mobile platform resulting in sharp increase in malware targeting the platform. Additionally, Android malware is evolving rapidly to evade detection by traditional

signature-based scanning. Despite current detection measures in place, timely discovery of new malware is still a critical issue. This calls for novel approaches to mitigate the growing threat of zero-day Android malware. Hence, the authors develop and analyse proactive machine-learning approaches based on Bayesian classification aimed at uncovering unknown Android malware via static analysis. The study, which is based on a large malware sample set of majority of the existing families, demonstrates detection capabilities with high accuracy. Empirical results and comparative analysis are presented offering useful insight towards development of effective static-analytic Bayesian classification-based solutions for detecting unknown Android malware.

Android permissions: a perspective combining risks and benefits

The phenomenal growth of the Android platform in the past few years has made it a lucrative target of malicious application (app) developers. There are numerous instances of malware apps that send premium rate SMS messages, track users' private data, or apps that, even if not characterized as malware, conduct questionable actions affecting the user's privacy or costing them money. In this paper, we investigate the feasibility of using both the permissions an app requests, the category of the app, and what permissions are requested by other apps in the same category to better inform users whether the risks of installing an app is commensurate with its expected benefit. Existing approaches consider only the risks of the permissions requested by an app and ignore both the benefits and what permissions are requested by other apps, thus having a limited effect. We propose several risk signals that and evaluate them using two datasets, one consists of 158,062 Android apps from the Android Market, and another consists of 121 malicious apps. We demonstrate the effectiveness of our proposal through extensive data analysis.

METHODOLOGY

- In this proposed system in order to improve the security of the mobile apps one methodology is proposed which will evaluate the mobile applications security based on the cloud computing platform and data mining. The task of identifying malware will be categorised into analysis, classification, detection and ultimate containment of malware.
- Several classification techniques are utilized in order to classify malware in keeping with their instances and this has created it potential to acknowledge the sort and activities of a malware and new variant. For such kinds of threats to mobile devices there should be some security mechanism to be implemented. Analysis of malware has got do with distinctive the instances of malware by completely different classification schemes by exploitation the attributes of well-known malware characteristics. Here also a prototype system named Malware detection system is presented to identify the mobile app's virulence or benignancy.
- Malware detection has to do with the quick detection and validation of any instance of malware in order to prevent further damage to the system. The last a part of the work is containment of the malware, which involves effort at stopping escalation and preventing further damages to the system.
- A commercial antivirus uses signature based mostly technique wherever the information should be often updated so as to possess the newest virus information detection mechanisms. However, the zero-day malicious exploit malware can not be detected by antivirus, supported signature-based scanner, however the utilization of applied math binary content analysis of file to detect abnormous file segments.

EXISTING SYSTEM

- The GP-PP (Generic Permissions-Privacy invasive permissions) model is useful to classify the permissions into Generic and Privacy invasive permissions. The model proposes a simplistic way for users to decide which apps are dangerous to install.
- Based on the permission set that a particular app requests, the GP-PP model classifies an app as privacy invasive if majority of the permissions requested are privacy invasive. So, users can decide which set of permissions can be harmful.
- We validate the GP-PP model in order to verify whether the model classifies an app on the basis of permission sets that the app requests.

DISADVANTAGES OF EXISTING SYSTEM

- Security is low.

PROPOSED SYSTEM

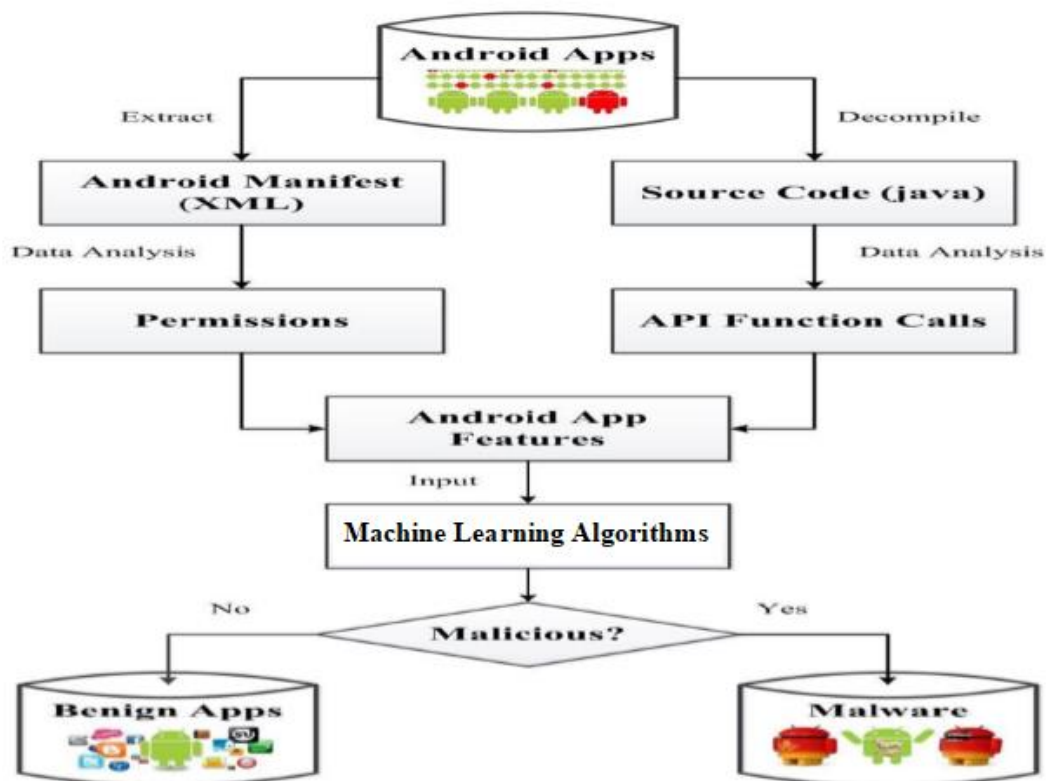
- Identify the list of third party installed applications.
 - Extract the complete list of permissions of each application.
 - Identify android: protection level of each permission, i.e. Normal or Dangerous of each app
-
- Take android app permissions dataset. To identify the harmful applications apply classification algorithms.

- Note the accuracy of spam classification given by it and time required for execution
- Results as accuracy among different harmful and normal apps Classifiers are analysed.

ADVANTAGES OF PROPOSED SYSTEM

- Security is high.

SYSTEM ARCHITECTURE



SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

System : Pentium Dual Core.
Hard Disk : 120 GB.
Monitor : 15"LED
Input Devices : Keyboard, Mouse
Ram : 1GB.

SOFTWARE REQUIREMENTS:

Operating system : Windows 7.
Coding Language : Android, Java
Toolkit : Android 2.3 Above
IDE : Eclipse/Android Studio

MODULES

- Login
- Application Download
- Android Permission Check
- Privacy Policy Database

LOGIN MODULE

This is the first activity that opens when user open the website. User needs to provide a correct contact number and a password, which user enters while registering, in order to login into the website. If information provided by the user matches with the data in the database table then user successfully login into the website else message of login failed is displayed and user need to reenter correct information. A link to the register activity is also provided for registration of new users.

Application Download

In this module, many application's are already download in mobile phone through play store. After installation just find the malware present in various application's.

Android Permission Check

A user who wishes to install and use any third party app doesn't understand the significance and meaning of the permissions requested by an application, and thereby simply grants all the permissions as a result of which harmful apps also get installed and perform their malicious activity behind the scene.

Privacy Policy Database

We presented a novel approach to the analysis of privacy policies in the context of Android applications. The tool we implemented greatly eases the process of understanding the privacy implications of installing third party apps and it has already been proven able to highlight worrisome instances of applications.

CONCLUSION

In this system, if your app handles personal or sensitive user data, please also refer to the additional requirements in the "Personal and Sensitive Information" section below. These Google Play requirements are in addition to any requirements prescribed by applicable privacy or data protection laws. We proposed, A user who wishes to install and use any third party app doesn't understand the significance and meaning of the permissions requested by an application, and thereby simply grants all the permissions as a result of which harmful apps also get installed and perform their malicious activity behind the scene.

REFERENCES

- [1] Yerima, S. Y., Sezer, S., & McWilliams, G. (2014). Analysis of Bayesian classification-based approaches for Android malware detection. *IET Information Security*, 8(1), 25-36.
- [2] Sarma, B. P., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., & Molloy, I. (2012, June). Android permissions: a perspective combining risks and benefits. In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies* (pp. 13-22). ACM.
- [3] Zhou, W., Zhou, Y., Jiang, X., & Ning, P. (2012, February). Detecting

repackaged smartphone applications in third-party android marketplaces. In Proceedings of the second ACM conference on Data and Application Security and Privacy (pp. 317-326). ACM.

[4] Chia, P. H., Yamamoto, Y., & Asokan, N. (2012, April). Is this app safe?: a large scale study on application permissions and risk signals. In Proceedings of the 21st international conference on World Wide Web (pp. 311-320). ACM.

[5] Yang, Z., Yang, M., Zhang, Y., Gu, G., Ning, P., & Wang, X. S. (2013, November) Appintend: Analyzing sensitive data transmission in android for privacy leakage detection. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (pp. 1043-1054). ACM.

[6] Zhang, W., Li, X., Xiong, N., & Vasilakos, A. V. (2016). Android platform-based individual privacy information protection system. *Personal and Ubiquitous Computing*, 20(6), 875-884.

[7] Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011, October). Android permissions demystified. In Proceedings of the 18th ACM conference on Computer and communications security (pp. 627-638). ACM.

[8] Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012, September). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (pp. 501-510). ACM.

[9] Mann, C., & Starostin, A. (2012, March). A framework for static detection of privacy leaks in android applications. In Proceedings of the 27th annual ACM symposium on applied computing (pp. 1457-1462). ACM.

[10] Stevens, R., Gibler, C., Crussell, J., Erickson, J., & Chen, H. (2012, May). Investigating user privacy in android ad libraries. In Workshop on Mobile Security Technologie

