# FRAUD APPLICATION DETECTION AND SUMMARY RISK SCORE

SHRADDHA JUNDHARE[1], PRIYANKA GADEKAR[2],PADMAJA GAJARE[3], ARCHANA AHER[4]

*(Department of Computer Engineering, Sinhgad Academy of Engineering, Maharashtra, India)*

*(Department of Computer Engineering, Sinhgad Academy of Engineering, Maharashtra, India)*

*(Department of Computer Engineering, Sinhgad Academy of Engineering, Maharashtra, India)*

*(Department of Computer Engineering, Sinhgad Academy of Engineering, Maharashtra, India)*

## ABSTRACT

*The prominence and usefulness of cell phones has made them appealing focuses for harmful and nosy applications. Android's current risk communication mechanism relies on users to understand the permissions that an app is requesting and to base the installation decision on the list of permissions. The users do not understand or consider the permission information as it requires technical knowledge. The Android's main safeguarding mechanism against malicious apps is the risk communication mechanism where usually any user installs the app, is being warned about the permissions the application would require and the user has to make the rightful decision. For mobile devices, one often downloads and uses many applications (or apps) with limited functionality from multiple unknown vendors. Therefore, the defense against malicious applications must depend to a large degree on decisions made by the users. An important part of malware defense on mobile devices is to communicate the risk of installing an app to users, and to enable the user to make informed decisions about whether to choose and install specific apps. We calculate the risk aggregate rating that users can use while choosing applications whether the user needs to use that app or not.*

**Keywords:-***Risk Score, Android Devices, NLP, Data Mining.*

## 1. INTRODUCTION

One of Android's fundamental safeguard mechanism against malicious applications is a risk communication system which, before a client introduces an application, cautions the client about the permissions the application requires, assuming that the client will settle on the right choice[2]. This approach has been appeared to be ineffective as it shows the risk information of each application in a "stand alone" design and in a way that requires a lot of specialized learning and time to distil helpful data[1]. We examine the wanted properties of risk signals and relative risk scores for Android applications keeping in mind the end goal to produce another metric that clients can use while picking applications[5]. We exhibit an extensive variety of procedures to create both risk signals and risk scores that depend on heuristics and also principled machine learning systems[1]. Trial comes about directed utilizing certifiable information sets demonstrate that these strategies can viably recognize malware as extremely unsafe, are easy to comprehend, and simple to utilize. One all the more thing, there are distinctive and immense number of applications on Play store[4], some of them look like same also by usefulness. Lot of applications are fake and can be fraud application. These may take information from your android device and may harm your android device anytime. Such applications additionally has client ratings and reviews by which we can figure out which one is fake or not. In an android application, we will have rundown of uses from various classes for which we can decide it is looked into as fake or not. Mobile vide access to individual and delicate data devices are getting to be omnipresent, and they item as telephone numbers, contact lists, geolocation, and SMS messages, making their security a particularly vital test[3]. For cell phones, one frequently downloads and utilizes numerous applications (or applications) with constrained usefulness from different obscure merchants. In this manner, the defennce against malicious applications must depend to a broad degree on decisions made by the clients[6]. An essential piece of malware protection on cell phones is to convey the danger of introducing an application to clients, and to empower the client to settle on educated choices about whether to pick and introduce particular applications.

## 2. ORGANISATION OF PAPER

While starting with literature survey, we will discuss the related work then proposed system with architecture and its test results. Then conclusion derived from the approaches we used and future scope of enhancement. At the end references used for preparing this paper are shown.

## 3. PROPOSED METHOD

The primary reason to build up the proposed framework for risk score functions for malware identified android applications. Given a risk score functions, one can develop risk signal by picking limit above which the threshold is raised. Such an approach supplements well different methodologies that attempt to recognize malicious applications. Each application hazard is counteracted in a way with the goal that it can be effectively compared with different applications. Our main aim is to provide application which will able to give more specific list of applications on play store using users reviews. Client needs to filter .apk records for identifying malware. We generate risk scores to improve risk communication for android apps[1]. For identification of client particular applications, proposed framework utilizes NLP and data mining calculation. We consequently propose the idea of risk scoring functions. Application is helpful for distinguishing fraud applications on Google play store, here to recognize misrepresentation applications proposed framework utilizes evaluations of clients for specific application. To break down clients reviews about applications, rate applications and give more related application on Google play store and in addition utilizing NLP examination recognize fraud applications.

## 4. FUNCTION MODULE AND ALGORITHMS

### 4.1 NLP:

Sentiment investigation otherwise called conclusion mining imply to the utilization of Natural Language Processing, content examination and computational linguistics to recognize and separate subjective data in source materials. Opinion investigation is generally connected to reviews and online networking for a variety of utilizations, running from showcasing to client benefit. As a rule, supposition examination expects to decide the state of mind of a speaker or an author concerning some theme or the general relevant extremity of a record. The disposition might be his or her judgment or assessment, full of feeling state, or the planned passionate correspondence (that is to state, the enthusiastic impact the writer wishes to have on the reader).Sentiment is not investigated through computerized reasoning, as a few people might be attract to think. Or maybe, it is examined by means of a deliberate procedure that includes the utilization of a supposition dictionary. Sentiment is not investigated through computerized reasoning, as a few people might be enticed to think. This is a method for examining opinion, then, by considering a sort of absolute energy or conflict of every word that would be utilized by somebody to discuss your business or items. For instance, "glad "would be regarded a positive word, and also "like" and "love".

### 4.2 System Architecture:

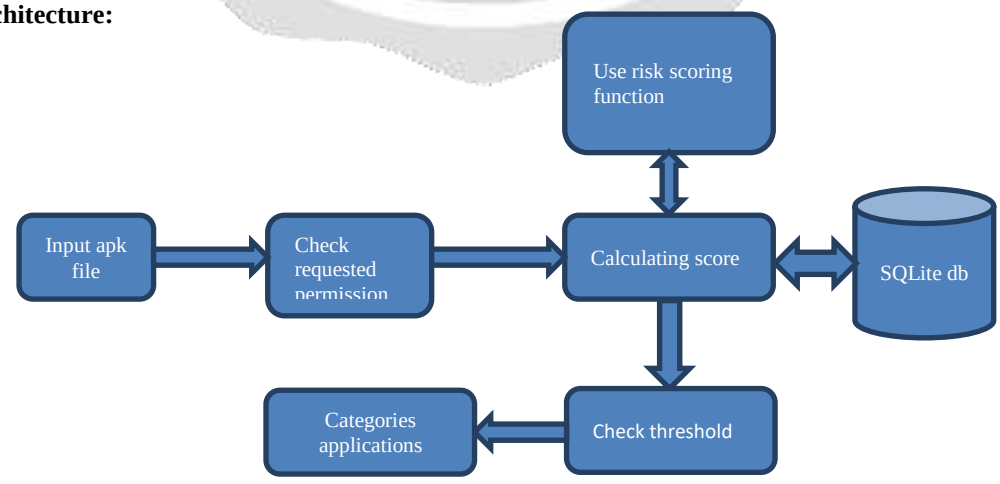



**Fig 1:** Summary Risk Score

## 5. IMPLEMENTATION

All components of the software need to be open source. The software must run on the Version android phone which runs the Android operating system. The mobile phone has existing hardware/software constraints. The database used by the software needs to be the same one that is used by the tools. The software must also use the language supported by the Android development environment, java plus the Android SDK. Android application development on either of the Microsoft Windows XP or later version..Linux including GNU C Library 2.7 or later.

- **Set-up Java Development Kit (JDK)**
  You can download the latest version of Java JDK from Oracle's Java site: Java SE Downloads. You will find instructions for installing JDK in downloaded files, follow the given instructions to install and configure the setup. Finally set PATH and JAVA_HOME environment variables to refer to the directory that contains **java** and **javac**, typically java_install_dir/bin and java_install_dir respectively.If you are running Windows and installed the JDK in C:\jdk1.6.0_15, you would have to put the following line in your C:\autoexec.bat file.

## 6. TEST CASES AND RESULTS

This project would be developed completely using open source software. So, anybody can use and enhance the software further without spending any money. Since all users are familiar with the general usage of computers, no specific training should be required to operate the system.
Our project virtual keyboard and mouse is implemented with the use of following software and hardware:

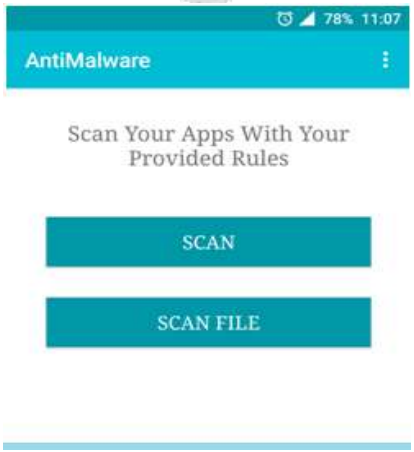
**6.1 Software Requirements:**

- Operating system: Windows version 7
- Language : Java, Android
- Software with version:
  1) Java 1.7
  2) Tomcat
  3) MySQL 5.6
  4) Android Studio 1.5
  5) Eclipse Kepler
- Database proposed: MySQL

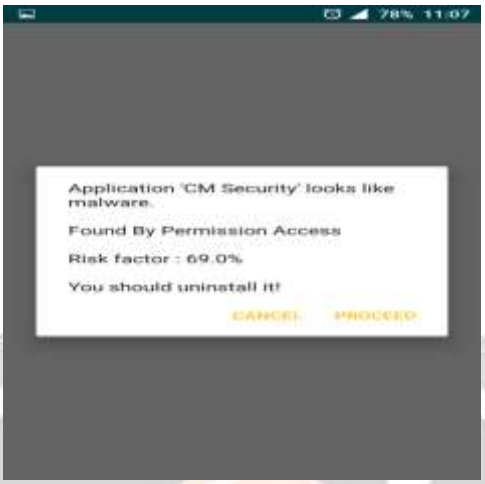
**6.2 Hardware Requirements:**

- 8 GB RAM
- 500 GB HDD
- Android Device

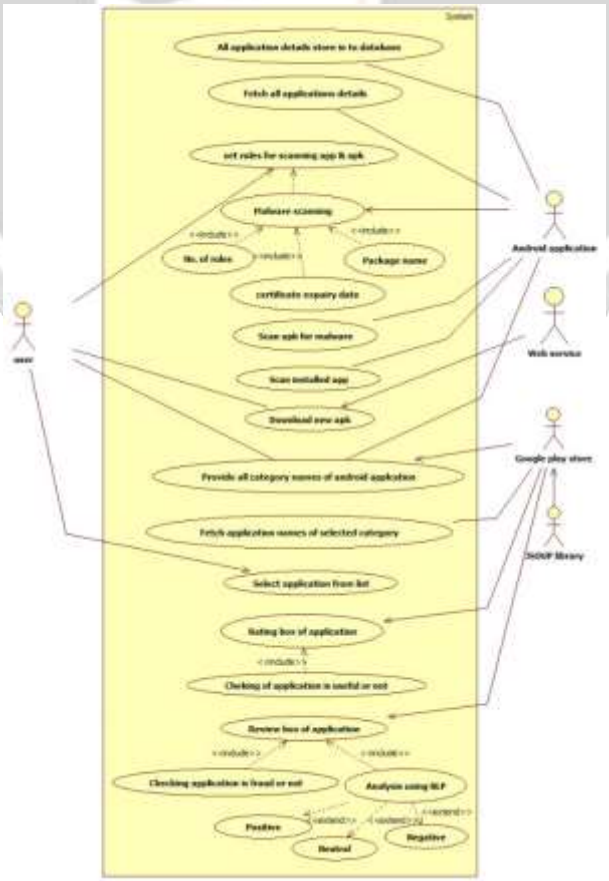
This is the user interface for Antimalware application. This application having a two buttons namely Scan and Scan file . By clicking on the Scan file button other activity will get displayed and where number of files are available .in this activity one can browse the various .apk files which are existing in the mobile.



The following image diplaying a dilougue box which shows the actual result related to risk score corresponding to that application.And also the warning sign related to that application




A use case diagram is a type of behavioural diagram defined by the Unified Modelling Language (UML) created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals represented as use cases and any dependencies between those use cases.



## 7. CONCLUSION

In this system, we build up the application for filtering applications and recognize malware. Structure incorporates both the irregularity based risk signals and probabilistic models. It also produces the chance scores to enhance risk communications for android applications.

Framework likewise gives more valuable application as indicated by client's reviews and recognize fraud applications as per evaluations. From this, we can conclude that proposed framework is valuable for identification of helpful applications and give enhanced risk communication.

## 8. ACKNOWLEDGMENT

I would like to take this opportunity to thank my internal guide Prof. ShaliniWankhade for giving me all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.

## 9. REFERENCES

[1] Christopher S. Gates, Ninghui Li, Senior Member, IEEE, Hao Peng, Bhaskar Sarma, Yuan Qi, Rahul Potharaju, Cristina Nita-Rotaru, 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

[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] 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.

[4] 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.

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

[6] 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.

[7] R. Stevens, C. Gibler, J. Crussell, J. Erickson, and H. Chen, "Investigating User Privacy in Android Ad Libraries," Proc. IEEE Mobile Security Technologies (MoST '12), 2012.

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

[9] AutoCog: Measuring the Description-to-permission Fidelity in Android Applications Zhengyang Qu1 , Vaibhav Rastogi1 , Xinyi Zhang2 , Yan Chen1 , Tiantian Zhu3 , Zhong Chen4 1Department of Electrical Engineering and Computer Science,Northwestern University, Illinois, USA 2Software School, Fudan University, Shanghai, China 3Software College, Northeastern University, Shenyang, China 4Wind Mobile,Toronto, Ontario, Canada.

[10] D. Barrera, H.G. Kayacik, P.C. van Oorschot, and A. Somayaji, "A Methodology for Empirical Analysis of Permission-Based Security Models and Its Application to Android," *Proc. 17th ACM Conf. Computer and Comm. Security*, pp. 73-84, 2010.

[11] "Andromaly": a behavioral malware detection framework for android devices. Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer, Yael Weiss.

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