Attack On Camera and Finding Fraud Applications from Play Store

[1]Chaskar Prachi D., [2]Dangat Pooja A., [3]Guldhekar Divya S., [4]Sukale Shubhangi

BE Computer, Department of Computer Engineering,
Jaihind Collage of Engineering, Kuran, Pune, India

***Abstract*: System focus on the security issues related to camera based attacks on smart phones. The fraudulent application and its traitor can be detected by using the defence system that detects the attacks. To evaluate the security system we have planned a camera based fraudulent application for utility study and also we analyzed the performance of the system with the fraudulent applications from the open android market. To download application smart phone user has to visit play store. When user visit play store then he is able to see the various application lists. This list is built on the basis of promotion or advertisement. User does not have knowledge about the application. So user looks at the list and downloads the applications. But sometimes it happens that the downloaded application won't work or not useful. That means it is fraud in mobile application list. We are going to find the applications those are fraud, from Google play store. We are providing sentiment analysis on the reviews, for finding true positive and false negative of the reviews and also working on NLP algorithm from which we are finding positive comments, negative comments and neutral comments..**

***IndexTerms*: Attacks, fraudulent, Google Play Store, NLP.**

I. INTRODUCTION

The Android operating system (OS) has enjoyed an incredible rate of popularity. Android OS holds 79.3 percent of global smart phone market shares. Meanwhile, a number of Android security and privacy vulnerabilities have been exposed in the past several years. Although the Android permission system gives user an opportunity to check the permission request of an application before installation, few users have knowledge of what all these permission requests stand for; as a result, they fails to warn users of security risks. Meanwhile, there are increasing number of apps specified to enhance security and protect user privacy have appeared in Android app markets. Most large anti-virus software companies have published their Android-version security apps, and tried to provide a shield for smart phones by detecting and blocking malicious apps. In addition, there are data protection apps that provide users the capability to encrypt, decrypt, sign, and verify signatures for private texts, emails and files. However, mobile malware and privacy leakage remain a big threat to mobile phone security and privacy.

Nowadays, people carry their phones everywhere; and, their phones see lots of private information. If the phone camera is exploited by a malicious spy camera app, there may occur serious security and privacy problems. Secret capturing photography is not only immoral but also illegal in some countries due to the invasion of privacy. Nevertheless, a phone camera could also provide some benefits if it is controlled well by the device owner. For example, when the owner wants to check if someone has used his/her phone without permission, the phone camera could be used to record the face of an unauthorized user. Besides, it can also help the owner find a lost phone. Can also use to take faster back up generation of the applications available in android system. And can be share easily with another user easily.

Different attacks on mobile phones can be done by the another user without user knowledge. These attacks can be detected and prevented by using this system. These attacks can be Attack on camera, Stolen mobile detection, tracking the location of the mobile system with the help Location tracking system, taking the faster back up of applications and can be share to another user, finding the applications which are fraud in Google play store. Finding spy app that will capture user image from camera without user knowledge. This attack can be done by the different application. So we need to find the applications those are fraud, from Google play store. Considering the Reviews given by the users which are given by them after using that application. When user visit play store then he is able to see the various application lists. This list is built on the basis of promotion or advertisement. User doesn't have knowledge about the application (i.e. which applications are useful or useless). So user looks at the list and downloads the applications. But sometimes it happens that the downloaded application wont work or not useful. That means it is fraud in mobile application list. Our system helps user to find out best application based on reviews and ranking. It gives download link to user for expected application.

II. PROBLEM STATEMENT

To resolve the issues and security breaches ,we have proposed an improved defence system with the ability to detecting the fraudulent application by considering the reviews with back up facility and also detect spy app that will capture the user image from camera without user knowledge.

III. MOTIVATION

- To evaluate the defense system we have proposed a camera based fraudulent application for feasibility study and also we analyzed the performance of the system with the fraudulent applications from the open android market.
- To download the application on smart phone user has to visit play store such as Google Play Store.

IV. PROPOSED SYSTEM

It is not possible to develop a system that makes all the requirements of the user. User requirements keep changing as the system is being used. Some of the future enhancements that can be done in that system

- As the technology emerges ,it is possible to upgrade the system and can be adaptable to desire environment .
- Because it is based on object-oriented design ,any further changes can be easily adaptable.
- Based on the security issues, security can be improved using emerging technologies.
- Face detection module can be added.
- Fraud app module can be added.

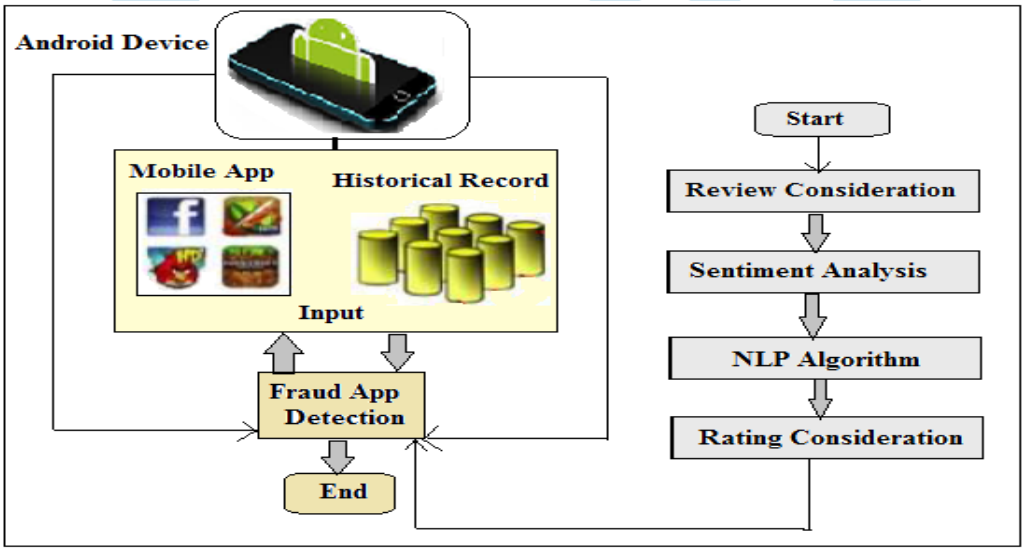


Fig. System Architecture

V. ALGORITHM

NATURAL LANGUAGE PROCESSING

Tokenization: Separate words into individual tokens and identify the class of the tokens. The difficulty of this task depends greatly on the complexity of the morphology of the language being considered.
Part-of-speech: Given a sentence, determine the part of speech for each word. Many words, especially common ones, can serve as multiple parts of speech.
Parsing: Determine the parse tree of a given sentence. The grammar for natural languages is ambiguous and typical sentences have multiple possible analysis.
Sentence Breaking: Given a chunk of text, find the sentence boundaries. Sentence boundaries are often marked by periods or other punctuation marks, but these same characters can serve other purposes.
Stemming: Separate a chunk of continuous text into separate words. For a language like English, this is fairly trivial, since words are usually separated by spaces.
Terminology extraction: The goal of terminology extraction is to automatically extract relevant terms from a given corpus.
Machine translation: Automatically translate text from one human language to another. This is one of the most difficult problems, and is a member of a class of problems colloquially termed ”AI-complete”, i.e. requiring all of the different types of knowledge that humans possess in order to solve properly.
Natural language generation: Convert information from computer databases or semantic intents into readable human language.
Natural language understanding: Convert tokens of text into more formal representations such as first-order logic structures that are easier for computer programs to manipulate.
Sentiment Analysis

Sentiment analysis refers to the use of natural language processing, text analysis and biometrics to systematically identify, extract, quantify, and study affective states and related information. Sentiment analysis is widely applied to customer materials such

as reviews/comments and survey responses, online and social media, and healthcare materials for applications that range from marketing to customer service to clinical medicine. Sentiment analysis use to determine the attitude of a commenter or other subject with respect to some topic or reaction to documents or applications, interaction, or event in the form of comments.

VI. MATHEMATICAL MODEL

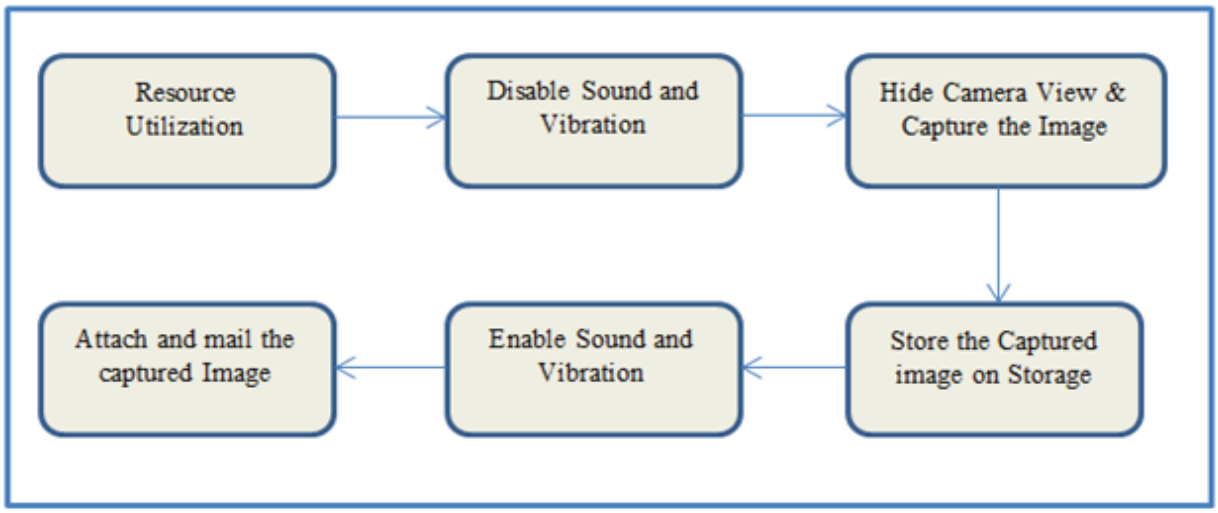
- Input: Application name for Fraud Detection, Access camera,.
- Output: Detect camera based attacks ,Finding fraud app successfully.
- Functions :
  Let S be the proposed system which can be represented as:
  S = I,F,Fi,O
  I1=Application name for fraud detection
  I2=Access camera
  F=Set of all processes
  O=Output
  I 1= F1,F2,F3,F4,F5,F6,F7
  F1= Application search
  F2=Review selection
  F3=NLP processing
  F4=Ranking based selection
  F5=Positive negative review
  F7=display download link
  I2=F11,F12,F13,F14,F15,F15
  F11=Resource utilization
  F12=Disable sound and vibration
  F13=Hide camera view and capture the user image
  F14=Store image in database
  F15=Enable sound and vibration
  F16=Attach and mail send
  O = O1,O2
  O1 = Detect camera based attack successfully
  O2 = Finding fraud app successfully
  S1=Application work properly

VII. SYSTEM MODULES

1. **User Registration** The users of the system have to firstly register with the application before going ahead and logging into it. The registration consists of firstly choosing the set of alphanumeric characters that the user desires for setting the password and User basic information i. e. Email-id, Name etc. For more security the user also gives a image password which will in turnbe hidden in the set of images that the user had selected. During logging in the user is asked to type the text password which is matched to the text which will be retrieved from the images which was stored during the registration.
2. **Camera Access Module** We use picture method of camera to detect attack on cameras. Our system check that when this method is called and by whom this method is called.
3. **Fraud App Detection Module** We have chosen some of them like Simple Notepad, Spy Camera, Hidden Camera, etc. We tested the feasibility of the improved defense system by opening the fraudulent applications. When the fraudulent apps started through the system, it will alert the user with a message along with detailed note. The alert will be in terms of a vibration and also voice clip. To detect the traitor of the fraudulent application which is proposed, we further doing a reverse engineering process to identify the mailing address from the package. The defense system is feasible than the mobile antivirus to detect the camera based attacks on Android phones.
4. **Review Ranking** In addition ratings, most of the App stores also permit users to write some textual comments as App reviews. Such reviews can indicates the individual perceptions and usage experiences of existing users for particular mobile Apps. Indeed, review manipulation is one of the most valuable perspective of App ranking fraud. Specifically, before downloading or purchasing a new mobile App, users usually first read its historical reviews to ease their decision making, and a mobile App contains more encouraging reviews may captivate more users to download..

VIII. RESULT ANALYSIS

It represents the operation of resource utilization .



Step 1:- Resource utilization by considering the power consumption, CPU and memory usage to intrude into the camera and gallery without users knowledge.

Step 2:- Setting flag 0 to sound and vibration.

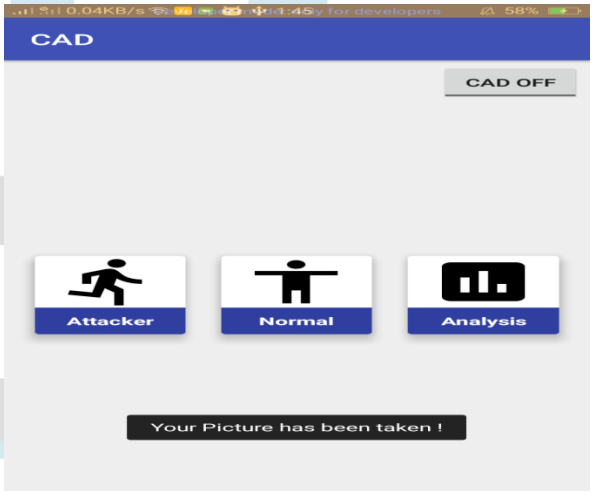
Step 3:- Hiding preview of the camera.

Step 4:- Capture the front camera and save in storage.

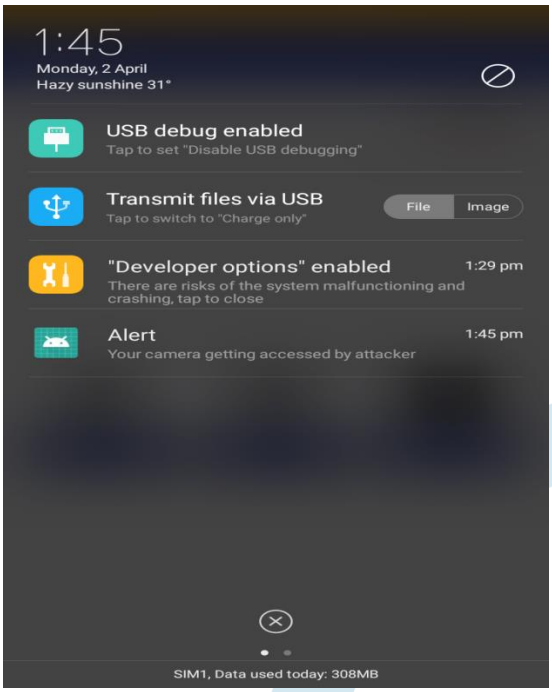
Step 5:- Recover the sound and vibration.

Step 6:- Send out the photo via mail.

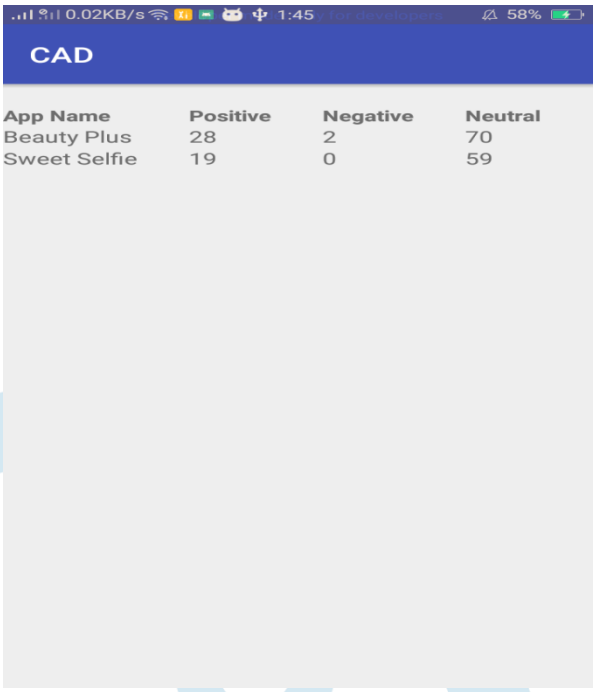
Dia. Camera Attack Detection



Dia. Normal Mode (Camera Attack Detection (CAD OFF))



Dia. Attack Prevented



Dia. Fraud Application Analysis

IX. CONCLUSION AND FUTURE SCOPE

Now day's lots of Android device used Android has very less restrictions for developer team, increases the security risk for People. Reviewed security issues in the Android based Smartphone. The integration of technologies into an application certification process requires overcoming logistical and technical challenges. Android provides more security than other mobile phone platforms. Moreover, in this project study camera-related accountability ,fraud apps and face detection in Android phones for mobile multimedia applications. We develop the system which plays important role that help to find detection of attack on camera that will benefit mobile users

In proposed system , which will investigate the feasibility of performing spy camera attacks on other mobile operating system .

REFERENCES

[1] Longfei Wu and Xiaojiang Du, Temple University Xinwen Fu, University of Massachusetts Lowell, Security Threats to Mobile Multimedia Applications: Camera-Based Attacks on Mobile Phones IEEE Communications Magazine March 2014.

[2] Ezra Siegel. Fake Reviews in Google Play and Apple App Store. Appentive, 2014

[3] Zach Miners. Report: Malware-infected Android apps spike in the Google Play store. PCWorld, 2014.

[4] Stephanie Mlot. Top Android App a Scam, Pulled From Google Play. PCMag, 2014 .

[5] Daniel Roberts. How to spot fake apps on the Google Play store. Fortune, 2015.

[6] Andy Greenberg. Malware Apps Spoof Android Market To Infect Phones. Forbes Security, 2014.

[7] Jon Oberheide and Charlie Miller. Dissecting the Android Bouncer. SummerCon2012, New York, 2012. VirusTotal - Free Online Virus, Malware and URL Scanner. https://www.virustotal.com/, Last accessed on May 2015.

[8] AsafShabtai, Uri Kanonov, Yuval Elovici, ChananGlezer, and Yael Weiss. Andromaly: a Behavioral Malware Detection Framework for Android Devices. Intelligent Information Systems, 38(1):161–190, 2012

[9] Michael Grace, Yajin Zhou, Qiang Zhang, ShihongZou, and Xuxian Jiang. Riskranker: Scalable and Accurate Zero-day Android Malware Detection. In Proceedings of ACM MobiSys, 2012

[10] BhaskarPratimSarma, Ninghui Li, Chris Gates, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy. Android Permissions: a Perspective Combining Risks and Benefits. In Proceedings of ACM SACMAT, 2012

[11] Chia-Mei Chen, Je-Ming Lin, Gu-HsinLai,National Sun Yat-sen University Kaohsiung, Taiwan "Detecting Mobile Application Malicious Behaviors Based on Data Flow of Source Code,2014 International Conference on Trustworthy Systems and their Applications.