**IOSR Journal of Engineering (IOSRJEN)** **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 39-43

# Detection of Malicious Apps In Android OS By Using Mobile Network

Dr Chetan J. Shelke, Mrs. Prajakta Shelke
*(Asst Professor,P.R.Pote College of Engg. and Mgmt.)*

***Abstract:*** *Malware is the mainly severe threats now a days many attack were launched using open platform android With the increasing significance of malware in Internetattacks, much research has concentrated on developing techniques to collect, study, and mitigate malicious Without confusion , it is compulsory to collect and study malware found on the mobiles . However, it is even more important to develop improvement and revealing techniques based on the insights gain from the study work. Thus developing malware finding approach that is both effective and well-organized, and thus, can be used to replace or set off traditional malware detection methods by using signature, permission as well user feedback methods.*

***Keywords:*** *malware, filter ,signature.*

## I. Introduction

Android phones are highly customizable and as such can be altered to suit your tastes and needs; with wallpapers, themes and launchers which completely change the glance of your device's interface. You can download apps to do all sorts of things like check your Facebook and Twitter feed, manage your bank account, order pizza and play games. You can plan events from your phone's calendar and see them on your computer or browse websites on your desktop Mac or PC and pick them up on your phone.[3]

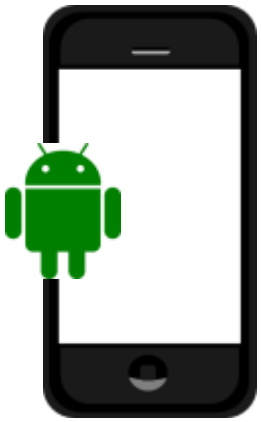


**Fig 1:** Smartphones and android[4]

Recent years have witness an explosion in the use of mobile computing thanks to the proliferation of feature-rich Smartphone's, and associated app stores and easy-to-install applications. Smartphone's have powerful hardware, with many useful sensors (e.g., GPS, camera, microphone, accelerometer) exposed via rich APIs, and enough computing power to run complex applications. The next generation of open operating systems won't be on desktops or mainframes but on the small mobile devices we carry every day. The openness of these new environments will lead to new applications and markets and will enable greater integration with existing online services. However, as the importance of the data and services our cell phones support increases, so too do the opportunities for vulnerability. It's essential that this next generation of platforms provides a comprehensive and usable security infrastructure [5]. Applications take advantage of these rich APIs to perform convenient and useful, but potentially privacy-sensitive tasks such as accessing address- book or location information; accessing online banking and medical accounts; and controlling home security systems. App stores make it easy for users to install and run applications, while providing few guarantees about their provenance or behavior. To protect sensitive resources from applications, and applications from each other, Android and other mobile OSes implement security mechanisms such as permission systems and strong isolation between applications. These mechanisms, however, have in practice proved insufficient, with an increasing number of malicious applications starting to target Smartphone's.

The number of mobile apps available for smart phones has grown exponentially in the last years. They are distributed by online stores such as the App Store for the iPhone and the Android Market for Android systems. The App Store makes a number of checks before making the applications available for download. Of course, the checks give some reasonable confidence that the applications run correctly but does not guarantee that they are immune to viruses and malware. The Android Market is using a different strategy that helps Android spread faster the online store is open without particular limits or quality checks to application developers that want to distribute and advertise their applications. Clearly, this makes Android an even easier target to viruses and malware[6].

## II. Literature Review

There are mainly two approaches to analyze the Android malwares: Static and Dynamic Approach.

### A. Static Approach

Static approach is a way to check functionalities and maliciousness of an application by disassembling and analyzing its source code, without executing the application. It is useful for finding malicious behaviours that may not operate until the particular condition occurs.

#### 1) Signature Based Approach

Signature based malware detection methods are commonly used by commercial antimalware products. This method extracts the semantic patterns and creates a unique signature. A program is classified as a malware if its signature matches with existing malware families‟ signatures. The major drawback of signature based detection is that it can be easily circumvented by code obfuscation because it can only identify the existing malwares and fails against the unseen variants of malwares. It needs immediate update of malware variants as they are detected.

#### 2) Permission Based Analysis:

In Android system, permissions requested by the app plays a vital role in governing the access rights. By default, apps have no permission to access the user‟ data and effect the system security. During installation, user must allow the app to access all the resources requested by the app. Developers must mention the permissions requested for the resources in the AndroidManifest.xml file. But all declared permissions are not necessarily the required permissions for that specific application.[8]

## III. Proposed methodology

Generally, the research work focus either on permission based detection or signature based detection for enhancing the malware detection or the combination of any two. Current malware detection mechanism return malware , but still fail to find true positive result every time. Most malware detection mechanism are deployed on mobile. So in this process, the user required extensive amount of battery and space, with the highly emerging use of smart phones .smart phones now a days able to perform various task as the cashless services are increasing day by day sensitive application such as banking related app rising danger due to malware attack its quite difficult and challenge to detect new malware In this article secured framework against application installation attacks on mobile network platform is applied. Parallel processing of three approaches i.e. user feedback filter, signature based detection filter and permission based filter. This system use j48 algorithm to find out the probability of malware.

To improve the detection mechanism framework is deployed on mobile network platform so to minimize the battery consumption as the space and processing speed of smartphones are limited. **Proposed** system firstly match the signature with signature database if the signature not match application check with permission as well as user feedback method by using J48 decision based tree method

1. Extract Signature,permission and feedback of Application(//sign from user level component)
if (sign = = matching sign from DB (//at mobile network component){
Declare Application as malicious
} else {
Go to Step 2
}
2. Match extracted permission on mobile network DB (//from user level component per IMEI)
3. Determine fgm ,fmm
4. If(fmm>fgm )
Go to step 5
Else

Go to next application and repeat above procedure
5. Check for the user feedback of application pf and pn (//from mobile network component)
6. If (nf>pf){
Declare Application as malicious
Else
Go to next application
7. Exit.
Where fgm = Permission match factor with genuine matching,
fmm = Permission match factor with malicious matching ,
pf= positive feedback &nf = negative feedback
As the step stated in approach of proposed system firstly all metadata are extracted from user level component i.e user feedback, permissions, and signature

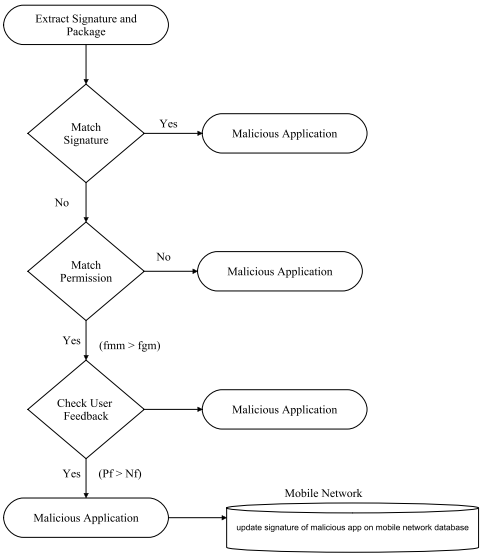
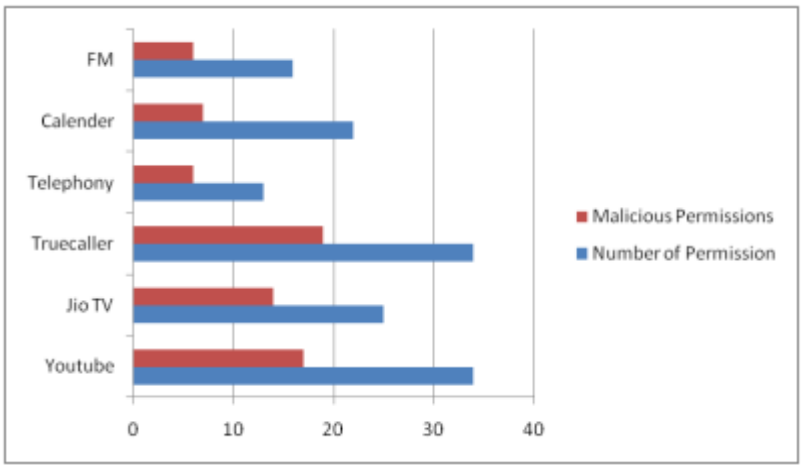



**Fig 2:** System flow of proposed system

## IV. Result Analysis

**Table 5.4:** Analysis of permission required by app

| Application | Permission Required |
|---|---|
| Youtube | 34 |
| Jio TV | 25 |
| Truecaller | 34 |
| Telephony | 13 |
| Calender | 22 |
| FM | 16 |




**Graph 5.4:** Analysis of permission required by app

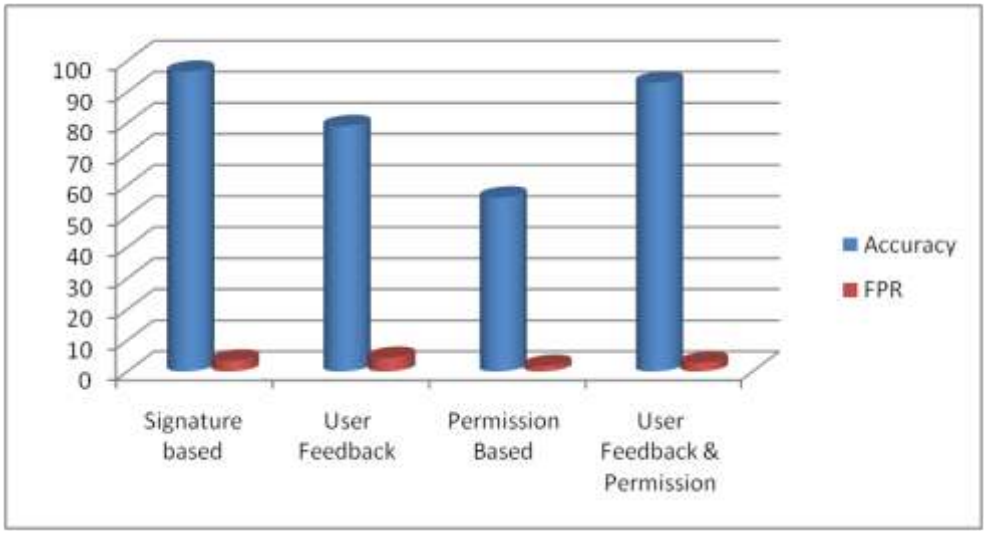
Graph shows the example of total number of permission and comparative analysis of malicious permissiontaken as per the permission based detection here the app FM, Colander, Telephony, jio and you tube are non malicious as they take less than 50 % ration of malicious permission and the app truecaller take more than 50%.so as per the permission based detection the application is malicious. As signature of true caller is not present in malicious signature set then the result of true caller is non malicious by signature based detection. also the system check for user feedback method the current analysis for true caller as per user feedback method is non malicious.The result of decision based tree j48 algo is suspicious

Malicious+non malicious=suspicious

Few test performed on implemented system by using 25 malicious app and 100 benign application on the mobile network and found that accuracy is not certain i.e. it differ by different application.

**Table 5.5 :** Accuracy for signature, user feedback, permission methods

| Sr. No. | Method | Accuracy | FPR |
|---|---|---|---|
| 1 | Signature based Detection | 96.5 % | 3.5 % |
| 2 | User feedback method | 79 % | 21 % |
| 3 | Permission based detection | 56 % | 44 % |
| 4 | User feedback &Permission based detection | 93 % | 7 % |




**Graph 5.5:** Analysis of signature,permission,user feedback method

$$AF = \frac{\text{Signature based} + \text{User feedback}}{2} \quad Permission\ based\ detection$$

$$Accuracyfactor = \frac{96.5 + 93}{2}$$

$$Accuracyfactor = \frac{189.5}{2}$$

$$\therefore Accuracyfactor = 94.75\ \%$$

## V. Conclusion

As Smartphone's devices are being rapidly utilized by enterprises, and various government agencies in addition in military services, security plays an important role, because many users uses these devices to hold their valuable sensitive data, attackers may use this sensitive information with wrong intent. Mobile malwarees can cause many types of reimbursement like, private data leakage, remote listening etc. also they can block the servers by sending many unnecessary messages and spam's and reduces the efficiency of communication network. that's why in order to control these malware attacks in Smartphone's some key steps must be taken to provide some efficient mechanism for controlling the growth and productions of these malwarees. The widespread use of virtualization into implement mobile network infrastructure brings unique security concerns for customers /tenants of a public mobile network service. A number of works have investigated these weaknesses from various perspectives, including demonstrating how applications can communicate through

covert channels, developing tools to detect information leaks, and implementing more powerful protection mechanisms. Providing better security policies is becoming most important area of research.

## References


[1] http://www.importantindia.com/24012/importance-of-mobile-phones-in-our-daily-life/
[2] https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile.aspx
[3] https://recombu.com/mobile/article/what-is-android-and-what-is-an-android-phone_M12615.html
[4] https://www.dreamstime.com/photos-images/android-logo.html
[5] M. Piercy, "Embedded devices next on the virus target list," in Electronics Systems and Software, vol. 2, no. 6, pp. 42-43, Dec. 2004- Jan. 2004
[6] M. V. Barbera, S. Kosta, J. Stefa, P. Hui and A. Mei, "CloudShield: Efficient anti-malware smartphone patching with a P2P network on the cloud," *2012 IEEE 12th International Conference on Peer-to-Peer Computing (P2P)*, Tarragona, 2012, pp. 50-56.
[7] Burguera I., Zurutuza U. and Tehrani S.N., Crowdroid: behaviour-based malware detection system for Android, 1st ACM workshop on Security and privacy in smartphones and mobile devices, 15-26 (2011).
[8] D. Dagon, T. Martin, and T. Starner, "Mobile phones as computing devices: The viruses are coming!" IEEE Pervasive Computing, vol. 3, no. 4, pp. 11–15, 2004.
[9] "F-secure",Available: http://Fsecure.com/what-is-Fsecure [Online, Access: 20 October 2014].
[10] Over a billion android-based smart phones to ship in 2017. Canalys, jun 2013
[11] Roman Llamas, Ryan Reith, and Michael Shirer. Apple cedes Market Share in smart phone operating system market as Android surges and Windows phone gains, according to IDC. http://www.idc.com /getdoc.jsp ?ContainerId =prUS24 257413 , Aug 2013