Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

FRAppE: Detecting Malicious Facebook Users

V. Sri Roja, A.Vineela, Y. Sri Sanjana, U. Prasanna Anjaneyulu
CSE & JNTUK, India

Abstract*: *Now a day's use of social networking site like Facebook for Communication and maintaining relationship among various users is increased due to its popularity on network. Each user that uses the social networking sites are making profiles and uploading their private information. These social networks users are not aware of numerous security risk included in this networks like privacy, identity theft and so on. The third party apps on social sites have main role to make the site more attractive. The hackers are using these third party users to get the private information and get unauthorized Access to their accounts. As we aware that not most but least of the applications on sites are malicious. As research goes on the research community has focused on detecting malicious wall-posts and Messages. In this paper, we are going to find that applications are malicious or not? In earlier system, Hackers have started taking advantages of the popularity of this third party apps platform and detecting malicious applications. There are many ways that hackers can benefit from a malicious app:(a)The app can reach large number of users and their friends to send messages and post pictures.(b)The app can obtain users personal information such as email address, Gender, etc.(c)The app can "re-produce" by making other malicious users popular. In proposed system , we can detect the persons who can post the images on our account by using "FRAppE". If anyone can send the spam messages more than a three times , Admin can detect and block the person who can send the spam messages .If the account is not a fake account then the person can send the message to the admin to unblock the account.

Keywords*— *Facebook Apps, Malicious Apps, Profiling Apps, Online Social Networks

I. INTRODUCTION

Online social networks (OSN) enable and encourage third party applications (apps) to enhance the user experience on these platforms.Such enhancements include interesting or entertaining ways of communicating among online friends, and diverse activities such as playing games or listening to songs. For example, Facebook provides developers an API that facilitates app integration into the Facebook user-experience. There are 500K apps available on Facebook, and on average, 20M apps are installed every day .Furthermore, many apps have acquired and maintain a large user base. Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications. Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Facebook leading the way with 900M active users. There are many ways that hackers can benefit from a malicious app: (a) the app can reach large numbers of users and their friends to spread spam, (b) the app can obtain users'personal information such as email address, hometown, and gender, and (c) the app can "re-produce" by making other malicious apps popular.

II. RELATED WORK

In this paper, we are going to find that applications are malicious or not? In earlier system, Hackers have started taking advantages of the popularity of this third party apps platform and detecting malicious applications.
There are many ways that hackers can benefit from a malicious app:
The app can reach large number of users and their friends to spread malwares.
The app can obtain users personal information such as email address,hometown,Gender, etc.
The app can "re-produce" by making other malicious apps popular.

III. EXISTING SYSTEM

In this paper, we are going to find that applications are malicious or not? In earlier system, Hackers have started taking advantages of the popularity of this third party apps platform and detecting malicious applications.
There are many ways that hackers can benefit from a malicious app:
The app can reach large number of users and their friends to spread malwares.
The app can obtain users personal information such as email address,hometown,Gender, etc.
The app can "re-produce" by making other malicious apps popular.

IV. PROPOSED SYSTEM

In proposed system , we can detect the persons who can post the bad videos and images on our account by using "FRAppE" .If anyone can send the spam messages more than a three times , Admin can detect and block the person who can send the spam messages.If the account is not a fake account then the person can send the message to the admin to unblock the account.

Procedure:

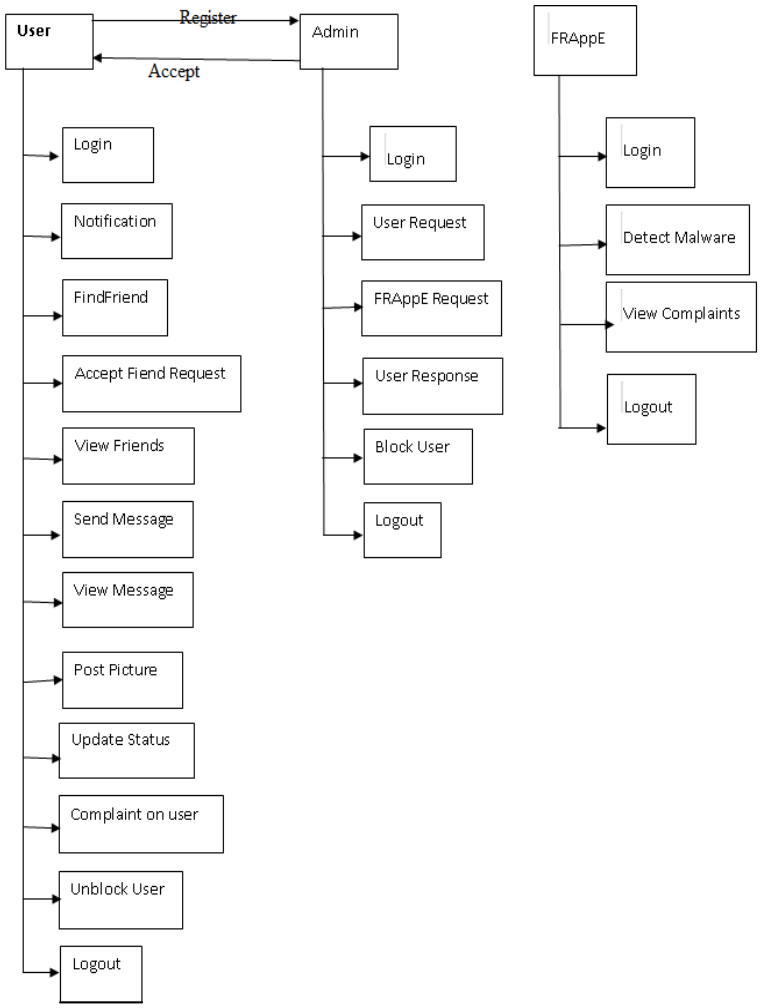
1) Registration: Thismodule provides the user to register himself/herself on the application by providing proper details , it will provide the user to enter into the Login Page.

2) FRAppE login: After registration the FRAppE can login using the Username and password .In this module FRAppE can detect malwares and complaints from the user and send to Admin.

3) Admin login: The admin logins to view the requests from the user. Based on proper verification he would be accepting the requests and also view the number of users. .In this Admin can block the user .

4) Logout: After completion of this procedure User,FRAppE,Admin will logout.

V. SYSTEM ARCHITECTURE



VI. RESULTS

Home Page

Complaint on user

Unblock User

Block User

VII. CONCLUSION

This Application performs about all the fake users who were existed in FRAppE. Here in Facebook it is a convenient process to Fake users for sending Messages and Posts on Facebook. However, a little is understood about this project of blocking users and how they unblock the users. In this process, large amount of Fake Users are involved. Fake users differ significantly to all other users with respect to several process. For example, Fake users are much more likely to send messages, post pictures with other users, So we develop FRAppE, a tool for "Detecting Malicious Facebook Users"between User and Admin. So that all the fake users can be de-activated and they can't login with their account.

VIII. FUTURE WORK

Already FACEBOOK Application is Existed in real time, but in this project we have enhanced with more reliable in detecting.Implement this project in Facebook for Real time.While the user is blocked, the Alert Message should exist on Email, So that user knows that he/she was Blocked.

REFERENCES

[1] 100 social media statistics for 2012. http://thesocialskinny.com/ 100-social-media-statistics-for-2012/.
[2] 11 Million Bulk email addresses for sale - Sale Price $90. http://www.allhomebased.com/ BulkEmailAddresses.htm.
[3] App piggybacking example. https://apps.facebook.com/mypagekeeper/ ?status=scam_report_fb_survey_scam_ Converse_shoes_2012_05_17_boQ.
[4] Application authentication flow using oauth 2.0. http://developers.facebook.com/docs/ authentication/.
[5] www.google.com

