ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.6

Detecting Malicious Account in Online Social Network using Proprietary Proguard Technology

W.Ancy Breen[1], M.Gowthami[2], P.Tamilselvan[3]
Assistant Professor[1, 2], PG Scholar[3]
Department of Computer Science and Engineering[1, 2], Master of Computer Applications[3]
Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai

Abstract:
In a recent time growing the usage of online social networks for example facebook. More number of people is using facebook in their daily life. So it leads to privacy, safety and security. Making friends in facebook and keeping in contact with them and seeing their update has become easier. But with their speedydevelopment, many problems like fake accounts, online imitation have also developed. There are no achievableresult exist to limit these difficulties. Here we proposed a ProGuard technique, it is used to analyze the behavior of the person in the facebook and the usage. The motive of this paper is to analyze the fraudfacebook profiles and also watermark techniques i.e., nothing but when a person shares a photo the other friend can also share the photo but that photo are not available for screenshots and downloads.

Index Terms: Facebook, ProGuard, Watermark

I.INTRODUCTION

In today's trend the online social networks simply called as OSN's like facebook, instagram, twitter allows the account holder to create their identity profile to update their activities to public, in personal profile to talk with their friends, family and colleagues. Also these networks are used for business promotions and communications. In statistical measures, the facebook is used by trillions of people and it becomes more famous and popular in the globe. The main usage of facebook is they can connect with their family and friends at anytime, anywhere by using internet connection. To mark the developing issue of harmful activities like spreading malware through OSN's so to solved this problems researchers have find a way that is to propose a ProGuard technique to detect fake accounts and fake activities and to safe people from malicious activities.

In the starting stage, the technique is used to detect the fake accounts that are automatically generated for the individual purpose. In facebook some sources will give fake rewards without knowing that the user will tempted to visit that malicious websites or else to install the applications and they share that post to their friends in facebook, thus licensing to spread viral. Unluckily, the recent proof visualizes thatbelieved sources are spreading malware and phishing attacks to gather the information. Recently, the popular Online Social Networks are the main target for phishing attacks so that they can attack more number of profiles and gather the data. Authorized users who lost their control regarding their account's activities then they can be named compromised account. So by phishing technique the spammer can collect the login credentials, without the legal user knowledge that user can spread the malware easily to others.

The main thing of this paper is to identify the fake accounts by searching the malicious accounts i.e. nothing but one person can creates the account with fake information and also they can send the request to anyone in facebook and then they can easily spread the malware by message or sharing post. Another attack is someone will offer fake gift rewards, vouchers which is used to install the malware applications and to spread it to their friend circle.Simultaneously, they can generate the duplicateprofile and they can act as a legal user like gathering the person's personal information like occupation, name, age, qualification etc., to identify and detect these kinds of techniques ProGuard techniques is introduced.

II.RELATED WORK

Identifying unwanted content and the advertisers that may be spammers who can makes a lengthy dare that influences on a daily basis.Uninvited or wrong messages can be sent to a more number of persons and it is said to be a spam and also it will used for a variety of usages and malware influences. Spam can be spread easily by advertising through televisions or else in paper and then spam calls has been a dangerous problem in modern communications with people. By using internet, the spammers reach the more number of people than previous measures. We can say that the old spam method is email spam.

In a recent time, Online Social Networks has given the chance to spammers to expand their spam messages in a effective medium. By utilizing social networks, spammers can impersonate themselves as legal users and they can participate in interactions. Simply the spammers can use this platform to send the messages on famous sources or pages, and replying to legal comments by utilizing the spam content. Such variety of chances has often enlarges spammers capability to secret their purposes from conventional filtering in spam. To end email spam and web spam content-based approaches is used and that is effective too. Not only in email and web spam, alsohave the

online social networks also enabled spammers to spread their spam contentin multiple messages in order to address the spam filters.Link-based approaches that grip the connection of theorganizations and that will unite with content based approaches are used to make it productive.

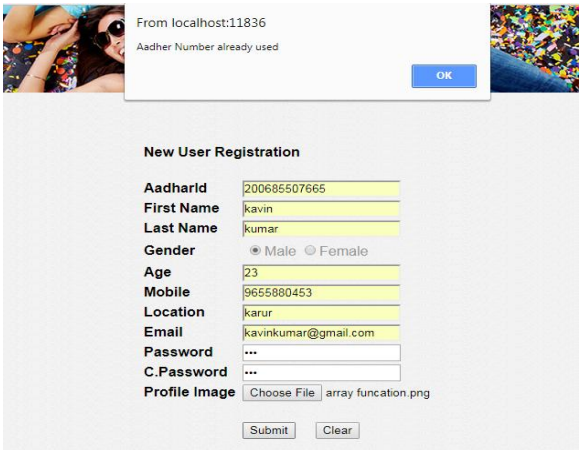
Furthermore, many online social networks cannot scan all the ordinary contents because of safety and privacy concern. Content unconventional structure it will be applied to the systems, that produces more safety and also with encryption process. More commonly, the structure is available to only multi-national OSN. The main aim is spot out the enlightening the spammers that demands manual or half-operated involvement by admin security.Starting stage in classifiers has been passed by spammers, so the spammers know how to operate their profiles and contents and to avoid filters that is automated. We visualize that our structure importantly decreases the requirement for admin to control the spamming. The usage of online social network damaged its responsiveness to malware.A online social network is organized for the users who has been already known each other only control the spam by avoiding the transmission between account holders who are not previously connected in the network. However, a online socialnetwork that encourages searching novel connections may wish to force limited work on how users interact.Also dare into the searching malware persons such as tagged is that account holders can united in the network for variety of reasons. For demonstrations, account holders can be tag to play the online games for entertainment. The research concentrated on detecting the spam in online social networks is relatively more in recent time. Correctively, to point out the malware problems and classify them into different kind of methods based on identifying and advancement. Based on the attention of the outcomes from the representation, the reliability system can generate flag a user as a malware person and deactivating theprofile or blocking its tasks in the model or else asking for more requirements.

III.SYSTEM MODEL

In the actual case we canachieve byidentifying the malicious account holder in online social networks particularly in business advancement activities by defeating the before declared challenges, so that we have introduced ProGuard technique. Itrecruits agroup of conducting features to view an account that contributes in an online promotion task

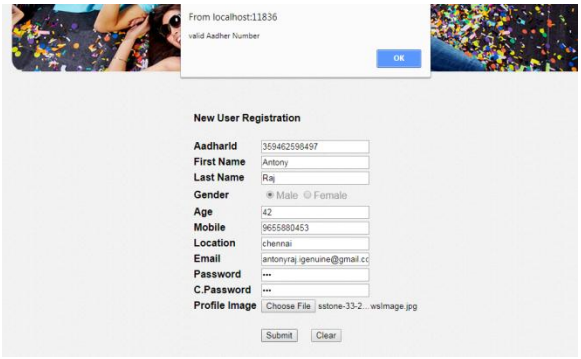
A. Identifying Malicious Accounts

ProGuardalsomerge these characteristics with a statistical categorizer so that they can be co-operatively used to differentiatewithin those accounts limited by intruders and good ones. For the best known, this work contributes the main action to consistently identifying malicious profilesutilized for online promotion activity involvement. The malware detection system is structured i.e. thesystem is able torecognizing malicious persons that involved in online promotion tasks for virtual moneygatheredthat are previously rewards are undertaken.

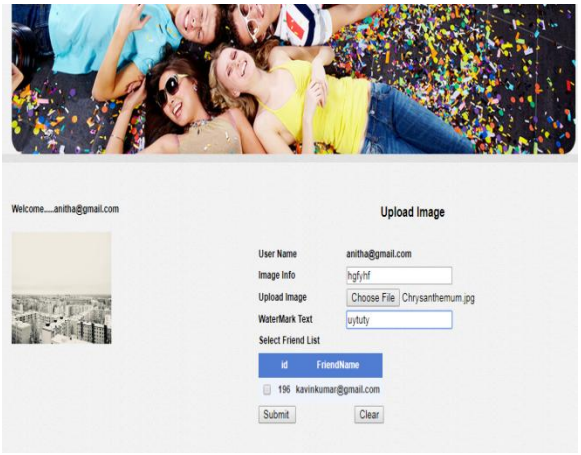


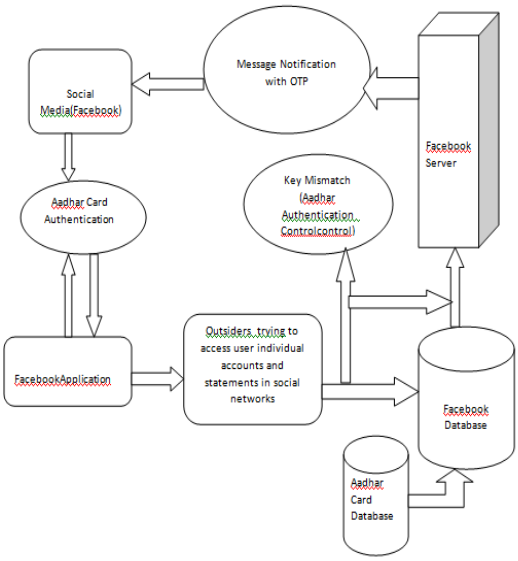
B. Spamming in Facebook

The account holder information like the username, the profile photo, occupation and the qualification are used to recognize the specific user.



In online social networks the details can be collected easily. To identify the same-site account, cloning will be used. By cloning process, the account which is having the same details for example name, qualification will be identified. Every online social network will give different kinds of social accounts which is having the similar details profile of the legal users will display.

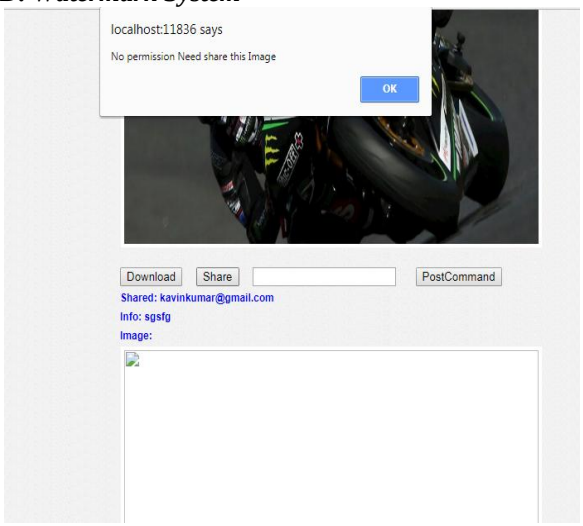




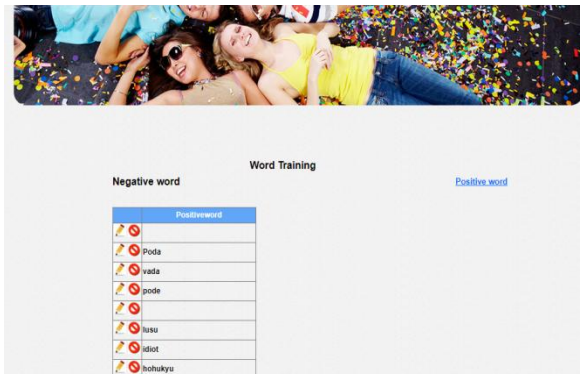
C. Brief Explanation of Architecture

In facebook application we can authenticate by using aadhar card details. When outsiders trying to access the user legal account and statements in online social networks, the facebook database will search for the aadhar card database, if the details are mismatch then it will control the authentication. If the details are matched then the facebook server will allows the account holder to enter into the account.

D. Watermark System



Watermark system is used to control the sharing of photos in facebook.



To prevent the attack from intruders this system is mainly used in this project.When the legal user share the photo in their profile as a profile photo or an event photo that image can be share by their friends. So that photo can visualize in front of the share account holder friend list, and then the photo can be shared by those persons also, in this case we use watermark system for the purpose not to download photos or to take screenshots.

IV.CONLCUSION

Extensive amount of uses of online social networks, the privacy and security issues will occur. To solve this issue this paper brings an approach as ProGuard Technique. The designing and implementation of this technique can identify accurately and efficiently fake accounts.Many times it is difficult to recognize the original post in facebook groups because more number of persons are sharing the posts daily for the transmission. To discriminate the legal and spam posts proposed technique is used. Functioning of this commencement is committed by receiving the outcomes utilizing this mechanism and this mechanism successfully detects the fake accounts.

REFERENCES

[1] NagaratnaHarikant, Suma V, "Risk Analysis in Facebook Based On UserAnomalous Behaviors" ICICCS 2017.

[2] Santa Barbara, Pittsburgh "COMPA: "Detecting Compromised Accounts on Social Networks".

[3]Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, Ben Y. Zhao "Detecting and Characterizing Social Spam Campaigns" *IMC'10,* November 1–3, 2010,

[4] Prateek Dewan, Ponnurangam Kumaraguru, "Towards Automatic Real Time Identification of Malicious Posts on Facebook" 2015 Thirteenth Annual Conference on Privacy, Security and Trust (PST)

[5] Tao Stein, Erdong Chen, Karan Mangla "Facebook Immune System" ACM Jan 1, 2011

[6] M.A. Devmane, Dr. N.K.Rana "Detection and Prevention of Profile Cloning in Online Social Networks" ICRAI E – 2014

[7]Yasmeen Sultana, Prof. B.I.Khodanpur,"Detecting the Malicious Application using FRAppE" ICICCS 2017