Detection of Malicious Applications on Facebook using Machine Learning Algorithm

Sneha C. Vishwakarma[1], Pooja R. Shejwalkar[2], Aishwarya R. Sadigale[3], Shyamal G. Palkhede[4], Prof. D. S. Thosar[5]

[1,2,3,4] *BE (Computer), Dept. of Computer Engineering, S.V.I.T, Chincholi, Nashik, Maharashtra, India*
[5] *Asst. Professor, Dept. of Computer Engineering, S.V.I.T, Chincholi, Maharashtra, India*

ABSTRACT

The usage of online social networking sites has become a integral part of our lives. It helps us to communicate with our dear and distanced ones. We can also use these sites for various media sharing purposes such as music, videos, etc. Also, these days these sites are gaining much more popularity due to the third party applications that exist on these platforms. However, intruders have realized the potential of these applications and use it as a medium to spam users. In a lot of cases, according to a survey done these applications are malicious. A spammer can benefit from these applications in various ways like, can reach a large number of users, can obtain user's personal information, and also with the help of a single user, he can spam a lot other users too. As the research goes on, research communities have focused on detecting malicious URLs and online social campaigns which are fake or spam. Here we develop an application, SecureU app, we help detect malicious application, fake or spam messages, hide pictures and posts which are inappropriate and it will also help us to give real time notifications.

Keyword: - *Malicious app, User Profiling Apps, Online Social Networks (OSNs), SQL Lite Database.*

1. INTRODUCTION

The existence of Facebook, Twitter or any other Online Social Networking Sites (OSNs) is a must in our daily lives. As it is way to stay connected and communicate with our closed and distanced ones. The sites are used for various purposes such as music, pictures, videos downloading, posting various photos, details etc. The addictiveness and craze of all these OSNs has increased due to the presence of the third party applications. However, the spammers have realized the potential of these third party applications and are using it as a tool to disturb and spam user profiles. Online Social Networking like Facebook witnesses an exponential increase in user activity. The activity is a combination of good quality content like information, personal views, opinions, comments etc. as well as poor quality contents like spam, other malicious contents. Spammers spread malicious posts trying to access the user personal information. We try to develop an application which detect whether given app is malicious or benign. We detect the app, if malicious it is shortlisted and user will be informed about the same. Also we provide real time notification to user and hence provide related security.

1.1 Motivation of the Project

A huge amount of masses use these social networking Medias as it provides us a way to express and share our views and interests with many others. These social platforms have on the other hand also can affect our lives in a bad way. A lot of information can be stolen and used for wrong purposes. These social sites have now become a popular platform for third party applications, which can be both malicious and benign. Spammers have realized the potential of these third party applications and use it to spam the users and gain their personal information. Hence, to provide the user security from these applications, we try to develop an application which detect whether given app is malicious or benign. We detect the app, if malicious it is shortlisted and user will be informed about the same. Also, we provide real time notification to user and hence provide related security.

2. LITERATURE SURVEY

Online Social Networking like facebook witnesses an exponential increase in user activity. The activity is a combination of good quality content like information, personal views, opinions, comments etc. as well as poor quality contents like spam, other malicious contents. Spammers spread malicious posts trying to access the user personal information.

Detecting malicious facebook users performs about all the fake users on facebook. In this process large amount of facebook users are involved. For example, fake users are more likely to send messages and post pictures. The tool developed for Detecting Malicious Facebook Users between users and admin [1].

Detecting malicious facebook applications, the security app called MyPageKeeper for facebook states that 60percent malicious apps get atleast 100,000 clicks on facebook. The review states to application mainly FRAppE and FRAppE lite. These malicious app detectors works on aggregation based features for cross verification of users like email id, gender, name etc. Used by facebook for third party applications that target large number of users [2].

Detecting malicious URLs using machine activity data, it is common for users to include URLs in their tweets to link to more detailed information, evidence, news reports and so on. URLs are often shortened do the endpoint is not obvious before a person clicks the link. Cyber criminals can exploit this to propagate malicious URLs on twitter, for which endpoint is a malicious server that performs unwanted actions on the person's machine. A machine classification system is developed to distinguish between malicious and benign URLs within seconds of the URL being clicked. Examine properties of learned model to explain relationship between machine activity and malicious software behavior [3].

We try to develop an application which detect whether given app is malicious or benign. We detect the app, if malicious it is shortlisted and user will be informed about the same. Also we provide real time notification to user and hence provide related security.

3. PROPOSED SYSTEM

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. The main aim is to protect oneself from social malware. One the user log in to the account the system works in the following manner: After log in, the user can upload any post he wishes to, this is then passed to a training set block. The next state is that of a feature extraction which checks the specified features which are stated by the SecureU application. Here, we use the SVM Algorithm as a classifier which consists of various parameters that are specified to identify the app, post, picture, etc. are malicious or benign.

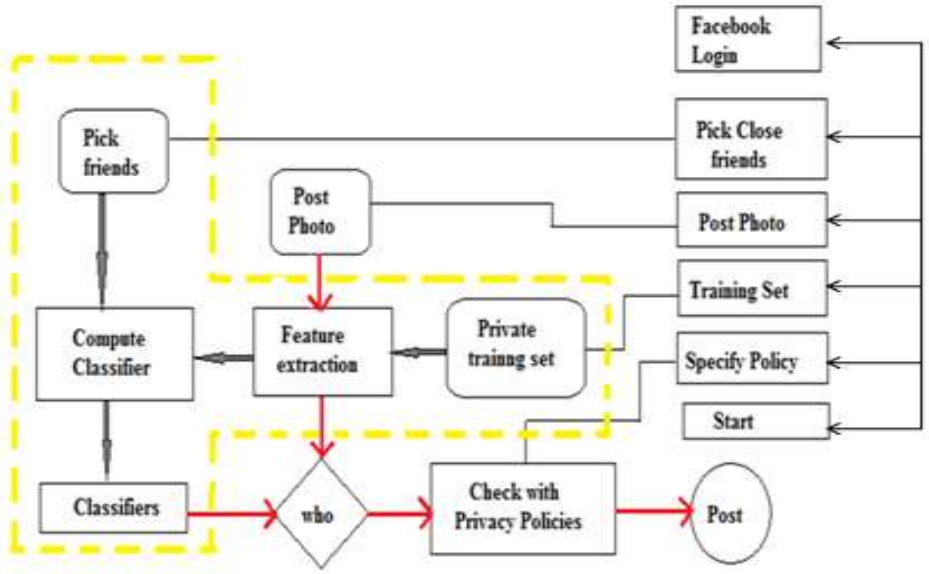

Fig-1: System Architecture

Facebook login:

Here the user login into his account, if the user does not yet register on facebook he can register his new account by providing various information like his email id, name, username, mobile number, etc. And if the user has already registered then he can directly login to his account.

Post photo:

User can post his image on facebook.

Training set:

Training set is a set of data used to discover potentially predictive relationships. The training phase consumes the training set, as other have pointed out, in order to find a set of parameter value that minimize a creation cost function over the whole training set.

Private training set:

We can train the classifier using 'training set', tune the parameters using 'validation set' and then test the performance of your classifier on unseen 'test set'. An important point to note is that during training the classifier only the training validation set is available. The test set will only be available during testing the classifier.

Feature extraction:

In machine learning, pattern recognition and in image processing, feature extraction start from an initial set of measured data and builds derived vales intended to be informative and non-redundant, facilitating the subsequent learning and generalization steps, and in some cases leading to better human interpretations. Feature extraction is related dimensionality reduction.

Compute classifier:

In these block we can compute classifier and can decide which classifier is to be used.

Classifier:

A classifier is a category of unified modeling language elements that have some common features, such as attribute or methods. A classifier describes a set of instance that have common behavioral and structural features.

3.1 System Description:

Function:

Detecting malicious applications
Providing real time notifications
Secure users friends too, by posting warnings on user's wall.

Input:

User login fields
Facebook as developer account
Project Application ID
Token of per user
Web services of User information

Output:

Detection of malicious applications successfully and adding it to our app.
Post warning on users wall.
Hide and prevent the sharing of bad posts and comments.
To determine whether the image is appropriate or not.

Success Conditions:

Availability of internet.
Application should be present on both sides.
Facebook account on both sides.

Failure Conditions:

If application is not present on either of the sides.
Unavailability of internet connection.

4. SNAPSHOTS

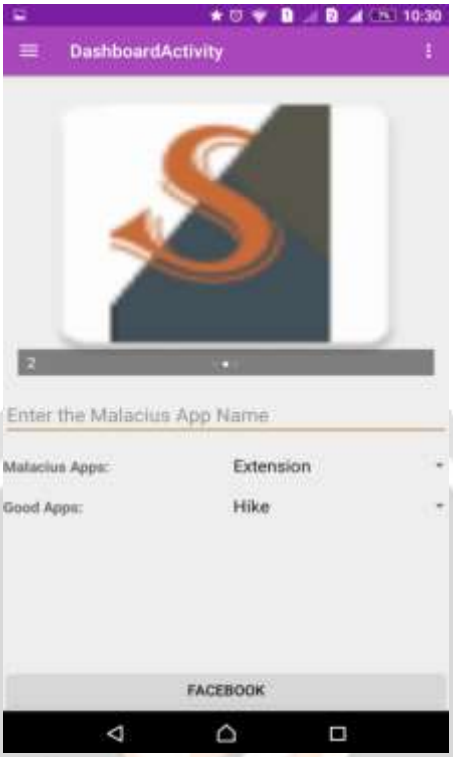

Fig-2: Enter app name to check whether malicious or not.

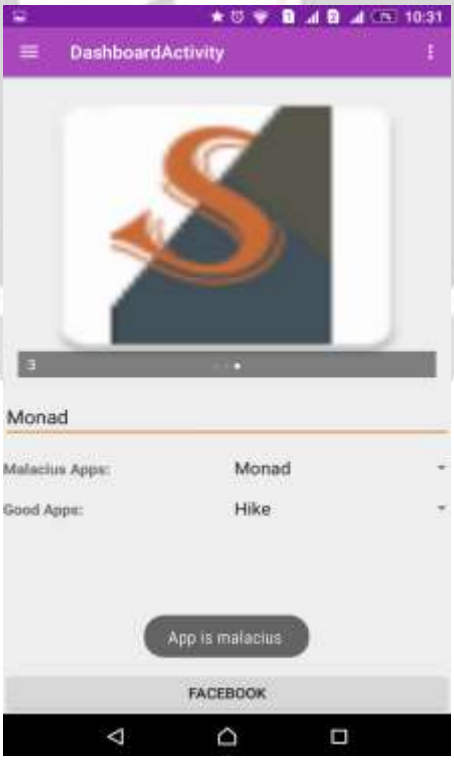

Fig-3: If app is found to be malicious, a message is displayed

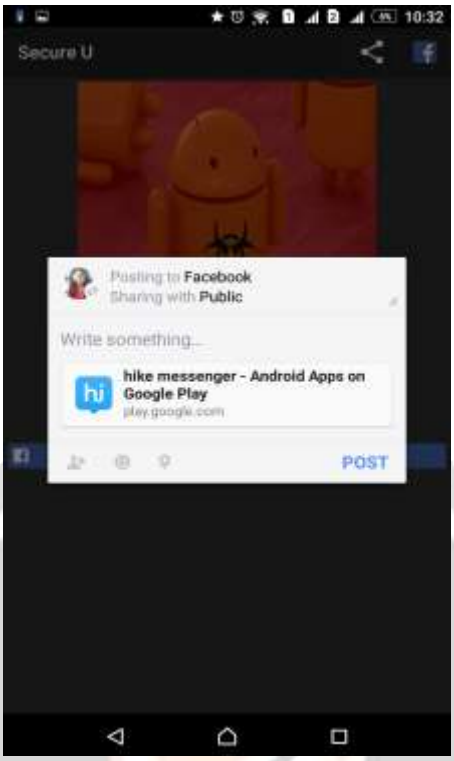

Fig-4: If app is not malicious it is successfully posted.

Fig-5: Sharing using other applications.

5. CONCLUSION

We have concluded that the application focuses on detecting whether an application is malicious or benign. It helps to keep the user secured from third party applications and also helps to hide bad posts, images and any other uploads. The work can be carried out on validation of a particular post, that is, for how long a post can be kept for a user to view. The posts whether images, comments can be filtered as good or bad and can be avoided from sharing.

6. ACKNOWLEDGEMENT

We take this opportunity to express our hearty thanks to all those who helped us in the completion of the project. We express our deep sense of gratitude to our project guide Prof. D. S. Thosar, Asst. Prof., Computer Engineering Department, Sir Visvesvaraya Institute of Technology, Chincholi for their guidance and continuous motivation. We gratefully acknowledge the help provided by them on many occasions, for improvement of this project with great interest. We would be failing in our duties, if we do not express our deep sense of gratitude to Prof. K. N. Shedge, Head, Computer Engineering Department for permitting us to avail the facility and constant encouragement. We would also like to thank Prof. R. B. Bhosale Project Co-ordinator for his great support and excellent guidance. We express our heartiest thanks to our known and unknown well-wishers for their unreserved cooperation, encouragement and suggestions during the course of this project report. Last but not the least, we would like to thanks to all our teachers, and all our friends who helped us with the ever daunting task of gathering information for the project.

7. REFERENCES

[1] Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, Michalis Falatous, “Detecting Malicious Facebook Applications,” In IEEE/ACM Transactions on Networking, 2015.

[2] V. Sri Roja, A. Vineela, Y. Sri Sanjana, U. Prasanna Anjanyulu, “FRAppE: Detecting Malicious Facebook Users”.

[3] Pete Burnap, Amir Javed, Omer F.Rana, Malik S.Awam, “Real Time Classification of Malicious URLs on TWITTER Using Machine Activity Data,” In IEEE/ACM International Conference on Advance in Social Network Analysis and Mining, 2015.

[4] Kiran Bhise, R. S. Shishupal, “Survey on Recognize Malignant Facebook Applications,” In Vol. 4, IJSR, December 2015.

[5] Yajin Zhou, Zhi Wang, Wu Zhou, Xixian Jiang. Hey You, “Get on My Market: Detecting Malicious Apps in Official and Alternative Android Market”.

[6] Application Authentication Flow using oauth 2.0. http://developers.facebook.com/docs/authentication.

[7] Microsoft. Security Intelligence Report. December 2013.

[8] A. Wang, “Machine Learning for Detection of Spam on Twitter Networks,” In proceedings of the 26th Annual Computer Security Applications Conference, ACSAC’2010, ACM.