INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

AN ENHANCED ALERT BASED SUSPICIOUS AND MALICIOUS APPLICATION BLOCKER SYSTEM IN SOCIAL NETWORK

K.L.Akshaya Nivasini[1], J.Jayapradha[2]

[1]M.E, CSE in Krishnasamy college of Engineering and Technology, E-mail:anujasri1192@gmail.com
[2]AP/CSE in Krishnasamy college of Engineering and Technology, E-mail:jpanandhi@gmail.com

Abstract: - With the advent of online social media, phishers have started using social networks like Twitter, Facebook, and Foursquare to spread phishing scams. Facebook is an immensely popular Social Media network where people use regularly with some third party applications in it. It has over 100 million active users who post about 200 million posts every day. Phishers have started using Facebook as a medium to spread phishing because of this vast information dissemination. Further, it is difficult to detect phishing on Facebook unlike emails because of the quick spread of phishing links in network, short size of the content, and use of URL obfuscation to shorten the URL. The technique is to detect phishing on Facebook in real time. In existing system this can be determine through FRAppE- Facebook's Rigorous Application Evaluator. FRAppE is the first tool focused on detecting malicious apps on Facebook. To develop FRAppE, we use information gathered by observing the behavior of Facebook apps seen across millions of users on Facebook. In addition to address these problems, proposed system use Facebook specific features along with URL features to detect whether a posts posted with a URL is phishing or not. Some of the Facebook specific features we use are post content and its characteristics like length, hashtags. The proposed system also uses machine learning classification techniques to classify the apps and detects phishing scams.

Keywords: Social network, Facebook Rigorous Application Evaluator, URL, Phishing Scams.

1. Introduction

A social networking service (also social networking site or SNS) is a platform to build social networks or social relations among people who share similar interests, activities, backgrounds or real-life connections. Users post content to the application to update connections and share personal news, accomplishments, interests and more. This content can be in the form of simple text status updates, videos or photos. Examples of social networks are LinkedIn, Facebook. However, social network users are not security experts and do not fully control their data.

Social networking sites have third party application in it. Third party applications are designed for the convenience of the users and to provide them all the features of the social networking sites and much more. People have become more addicted to these kinds of third party application. By using these applications hackers easily obtain the user information. It is over hard to handle privacy threats in third party application. In older

methods they concentrate only on detecting the suspicious URL and detecting the malicious application but not concentrate on blocking the malicious application. The evolution of URL can take lot of time. To detect the malicious, various methods and algorithms are used, but these were ineffective because of loss of security. To overcome the above problem, machine learning classification and offline supervised algorithm is proposed. In addition blacklisting mechanism can be used. By using this mechanism it filters the unsolicited messages too.

This algorithm and techniques plays a major role in classify the application and block the application. When the application tries to hack the user information, the techniques classify the application and check whether the application is malicious or not. These techniques put a stop to hacking of information which means that certain apps does not immediately hack the information for an undetermined period of time.

2. Existing system

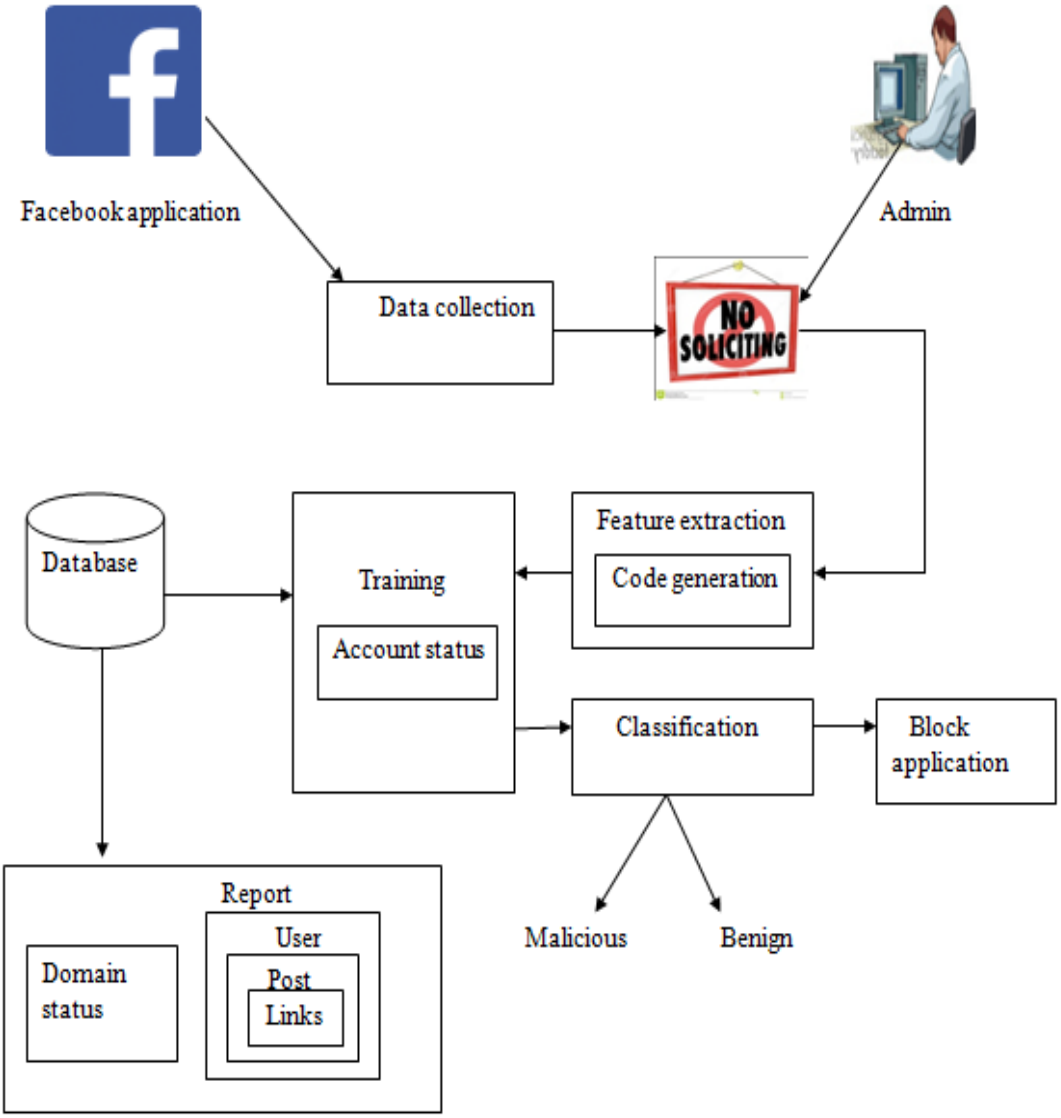
In existing system malicious apps can be determined by FRAppE and FRAppE Lite. FRAppE use information gathering and it detect the malicious apps with 99.5% accuracy, with no false positives and a low false negative rate. FRAppE is a malicious application detector that uses both On-demand features and aggregation based features whereas FRAppE Lite uses only on-demand features, it include Application summary, required permission set, Redirect URL, Client ID in app installation URL, Posts in app profile. Aggregation-based features includes App name, External link to post ratio. FRAppE Lite can identify malicious apps with 99.0% accuracy, with low false positives (0.1%) and false negatives (4.4%).

FRAppE Lite is a lighter weight version when compared to FRAppE so FRAppE is considered better than FRAppE Lite.To build FRAppE, it use the data from MyPageKeeper.MyPageKeeper is a security application that monitors the profiles of 2.2 million users. MyPageKeeper primarily relies on SVM that evaluates every URL by combining information obtained from all posts containing that URL. MyPageKeeper indicate all posts containing the URL as malicious. Malicious application is characterized by certain factors such as malicious applications either have no post or it may have too many posts but it redirect to the malicious URL. Malicious apps do not operate in isolation in the sense many malicious application can share the same name, same domain upon installation, etc.Existing system has several limitations such that it crawls only a portion of application but collecting an ideal large set of datas is an impossible mission.

3. Proposed approach

Malicious application will be determine through the technique of machine learning classification. It is a classifier that classifies the application and it is a *supervised* statistical classification. Supervised because the system needs to be first trained using already classified training data as opposed to an unsupervised system where such training is not done. The first step is that it determines the type of training. The second step is it gathers a training set. The training set needs to be representative of the real-world use of the function. Thus, a set of input objects is gathered and corresponding outputs are also gathered, either from human experts or from measurements. The third step is determining the input feature representation of the learned function. The accuracy of the learned function depends strongly on how the input object is represented. Typically, the input object is transformed into a feature vector, which contains a number of features that are descriptive of the object. The number of features should not be too large. The fourth step is determining the structure of the learned function and learning algorithm. The final step is complete the design and evaluate the accuracy of the learned function. System considered the individual URL instead of group of URL. To deny the third parties, feature can be extracted based on random number generation algorithm. It is also based on yarrow algorithm which it generates the secure pseudorandom number. This random number is unpredictable to the attacker because it a multiple dynamic numbers generator. Then it uses the blacklisting mechanism that filters the unsolicited messages in order to enhance more security. BL is directly managed by the system, which should be able to determine who the users to be inserted in the BL. To enhance flexibility, such information is given to the system through a set of rules, hereafter called BL rules. Such rules are not defined by the Social Network Management, therefore they are not meant as general high level directives to be applied to the whole community. Rather, we

decide to let the users themselves, i.e., the wall's owners to specify BL rules regulating who has to be banned from their walls and for how long. Therefore, a user might be banned from a wall, and at the same time, he/she will not be able to post in the wall. Thus, proposed system enhances more security as well as it provides step by step authentication. Also it concentrate on stop the redirect of URL which means it does not associated with the hackers to hack the user information.

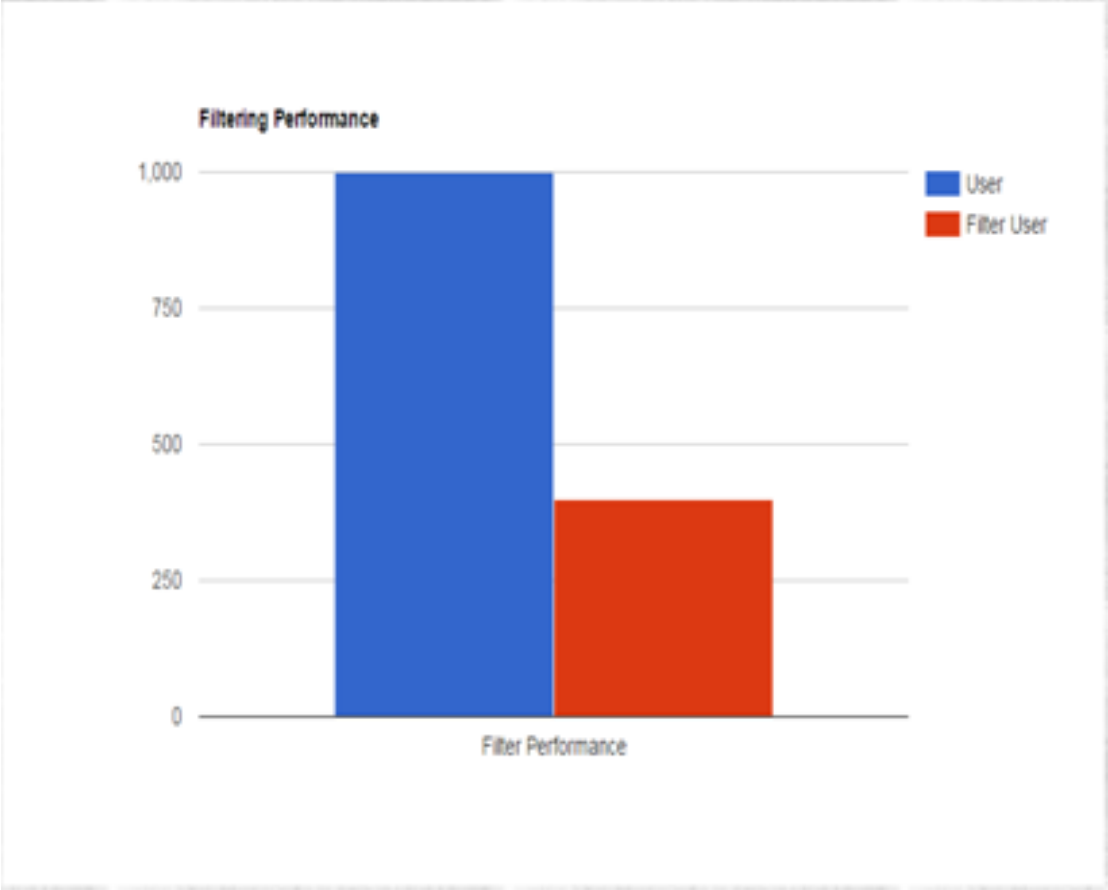


3.1 Applications

- Verification of application to enhance security.
- To stops the unsolicited messages.

4. Performance evaluation

Consider number of users accessing the application. From that we can allow only the authenticated/authorized user by considering the several characteristics. The following chart shows the filtering performance of the application.



5. Conclusion

To identify and block the malicious application various methods and algorithms are used, but these were ineffective because of loss of security. In this paper, a system to prevent the indecent messages from the social networking site walls has been presented. The usage of blacklisting mechanism automatically filters the unsolicited messages and the usage of code generation algorithm provides multiple codes that deny the access of application by hackers. By using this it provides more security. Admin can collect the user information. It also concentrates on verifying whether the user is authenticated or not by generating the code. Admin. can also track the user information in order to provide more security. In addition admin can maintain the user information for an undetermined time period. And finally it blocks the malicious application by considering certain features. They initially train the system by using the supervised algorithm. It mainly focused on providing the step by step security verification and it provides the activation code to enter into application, sharing photos and so on. By the code generation, the hackers cannot access the other user account or the user does not post the images and so on. The future work focus on the effective implementation of blocking system which it will block the malicious application and it will protect the application from hackers. Nowadays users are unaware of revealing the personal information to others. For this, future work mainly concentrate on preventing the revealing the user information by blocking the malicious application. One of the ways to hack the user information is spread the phishing scams and through this scams hackers easily hack the information. Thus the system stops the spreading of phishing scams and blocks the malicious application too.

By doing this, they also stop the redirect of URL and overcome the problems which are faced by users in most OSN presently. And our future works overcome the deficiency of both the aggregate features and on demand features. Based on these features it classifies the abnormal applications and benign applications and thus it finally blocks only the malicious applications.

REFERENCES

[1] M. Gjoka, M. Sirivianos, A. Markopoulou, and X. Yang.Poking facebook: characterization of osn applications. In Proceedings of the first workshop on online social networks, WOSN, 2008.
[2] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker. Beyond blacklists: learning to detect malicious web sites from suspicious urls. In KDD, 2009.
[3] A. Besmer, H. R. Lipford, M. Shehab, and G. Cheek. Social applications: exploring a more secure framework. In SOUPS, 2009.
[4] A. Makridakis, E. Athanasopoulos, S. Antonatos,D. Antoniades, S. Ioannidis, and E. P. Markatos.Understanding the behavior of malicious applications insocial networks. Netwrk. Mag. of Global Internetwkg., 2010.
[5] Md Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos,"FRAppE: Detecting Malicious Facebook Applications", in networking, vol: pp no: 99, 2015.

Author's profile

K. L. AKSHAYA NIVASINI is presently pursuing her M.E degree in computer science and engineering at Krishnasamy College of Engineering and Technology, Tamilnadu, India. She has received her B.E degree in CSE from Krishnasamy College of Engineering and Technology, Tamilnadu, India. Her research interests are in the areas of Mobile computing, Networking.

J. JAYAPRADHA received B.E CSE degree from Dr.Pauls Engineering College and M.E CSE degree from Hindustan College of Engineering and Technology. She is working as Assistant Professor in the department of computer science at Krishnasamy College of Engineering and Technology, Cuddalore, Tamilnadu, India. Her research interests are in the areas of Operating system, Compiler design, and Distributed system.