Detecting Malicious Activity in Facebook Application

Md. Shoaib[1], Anas Ahmad[2], Rohit Kshirsagar[3], Prof. Sunil Deokule[4]
[1, 2, 3, 4] Shree Ramchandra College of Engineering Lonikand, Pune -412216

Abstract- *The aim of this system is mainly to provide users a filtering mechanism to avoid their walls overwhelmed by useless data. Due to the fact that in FACEBOOKs there is the possibility of posting or commenting other posts on particular public/private areas. Information filtering can therefore be used to give users the ability to automatically control the messages written on their own walls, by filtering out unwanted messages. We have implemented an automated system, called ConnectifyMe, able to filter unwanted messages, images from FACEBOOK user wall. The images posted on the FACEBOOK wall which may contain vital information hidden in it, which leads to terrorist activities. For Filtering the images we provide a steganography mechanism that decodes the hidden data, making it more secure. There are possibilities of getting phishing links on the FACEBOOK walls, thus to alert the user about the phishing link, system is using an anti-phishing algorithm called obURL, which has six different steps to filter the link and alert the user if phishing site is detected.*

Keywords- filtering OSN user wall, message filtering, steganography, phishing link.

I. INTRODUCTION

As we know, these days everyone seems to be victimization On-line Social Networks (OSNs) to speak and share data. Therefore, one vital want in these days On-line Social Networks (OSNs) is to offer users the power to manage the messages denote on their own personal area to avoid that unwanted content is displayed. We have implemented an automated system, called ConnectifyMe, able to filter unwanted messages, images from FACEBOOK user wall. As we know that FACEBOOK walls are overwhelmed by huge number of messages, comments that are posted by their friends and friends of friends. There are also some vulgar, unwanted messages been posted on user wall which harms image of the user. It is a hectic process to delete such messages & comments each and every time. In our system we are providing user the filtering mechanism through which user can give filter patterns according the messages are filtered on the FACEBOOK wall. The friends whoever have posted such messages are blacklisted for duration of time. If a friend posts such messages more than three times he/she blocked automatically and notifications is provided to both the sender and receiver of messages. Phishing links that lead user to mislead and hacking of users credential data. We are providing phish link detection through Link Guard Algorithm which alerts the user from phishing link. As OSN being target for terrorist activities, secret messages are hidden in images and spreading them through the social media so that they are not detected easily. To restrict such activist we have implemented the steganography which will filter the images and decode the hidden message in it.

II. LITERATURE SURVEY

Online Social Networking is the application associated with the email address of the user. It contains different functionality of chatting, posting messages, update status, adding friends and many more. Some of the examples are Facebook wall, Twitter etc. When a message is delivered to a local user of Mail Server, it is stored in the INBOX folder. In Web Mail, each user can define a set of actions to be performed on all new incoming messages, as well as their conditions. These actions are called filters and are specified through filtering rules. Filtering does not mean merely refusing email messages or sorting them to folders, but it includes other actions such as notifications, automatic replies, forwarding the message to a different email address, etc. The term phishing is a general term for the creation and use by criminals of emails and websites designed to look like they come from well-known, legitimate and trusted businesses, financial institutions and government agencies–in an attempt to gather personal, financial sensitive information. These criminals mislead Internet users into disclosing their bank and financial information or other personal data such as usernames and passwords, or into unknowingly downloading malicious computer code onto their computers that can allow the criminals subsequent access to those computers or the users' financial accounts.

III. MODULES TO BE IMPLEMENTED

ConnectifyMe is the system which provides a secure way to handle the OSN wall and its related difficulties.

The system able to filter out unwanted messages, images and links from social network user walls.

A. OSN user wall

In this module first we can create user GUI like user can login with our application by adding his personal information like his name, password, address etc.

a) User Registration (Sign In / Signup)

In this module first user register with our application by adding his personal information like his name, password, address and his hobbies etc. After registering with our application he can login with us using userid and password.

b) Adding / Inviting Friends

After login into the system a user can add friends by seeing there profiles, in this module user sends requests to the friends when user accepts the request, he becomes his friends. Also user can Invite friends regarding any invent.

c) Chatting / Messaging

After adding friends user can see online friends and select a particular friend for chatting.

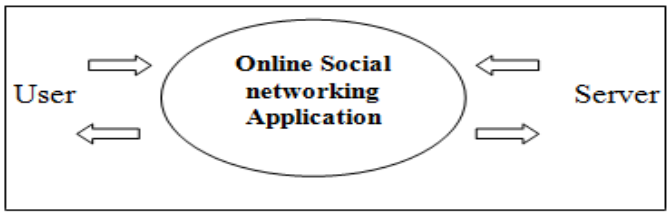

Figure 1: Data flow diagram 0

In above data flow diagram a simple connectivity between user and server are shown.

d) Post on User wall

User can update his status on his wall, all his friends can see this status and post there view about your status. So this message should get filtered. So we are implementing here filtering rules.

B. Filtering Pattern

In defining the language for FRs specification, we consider three main issues that, should affect a message filtering decision. First of all, in OSNs like in everyday life, the same message may have different meanings and relevance based on who writes it. As a consequence, FRs should allow users to state constraints on message creators. Creators on which a FR applies can be selected on the basis of several different criteria; one of the most relevant is by imposing conditions on their profile's attributes. In such a way it is, for instance, possible to define rules applying only to young creators or to creators with a given religious/political view. Given the social network scenario, creators may also be identified by exploiting information on their social graph. This implies to state conditions on type, depth and trust values of the relationship creators should be involved in order to apply them the specified rules.

C. Image Filtering

In this we are using the LSB algorithm to filter the images and decode the text from the images and display it. In this we are avoiding the misuse of Social Networking by the terrorist to pass their secrets messages through images.

D. Phishing prevention for links posted on user walls

Phishing is a new word produced from 'fishing', it refers to the act that the attacker allure users to visit a faked Web site by sending them faked e-mails (or instant messages), and stealthily get victim's personal information such as user name, password, and national security ID, etc. This information then can be used for future target advertisements or even identity theft attacks (e.g., transfer money from victims' bank account). So we are providing here an anti-phishing environment for the links posted on user wall.

IV. SYSTEM ARCHITECTURE

Three Tier architecture is used in OSN services. These three layers are

A) Social Network Manager (SNM)
B) Social Network Application (SNA)
C) Filtered Wall (FW)

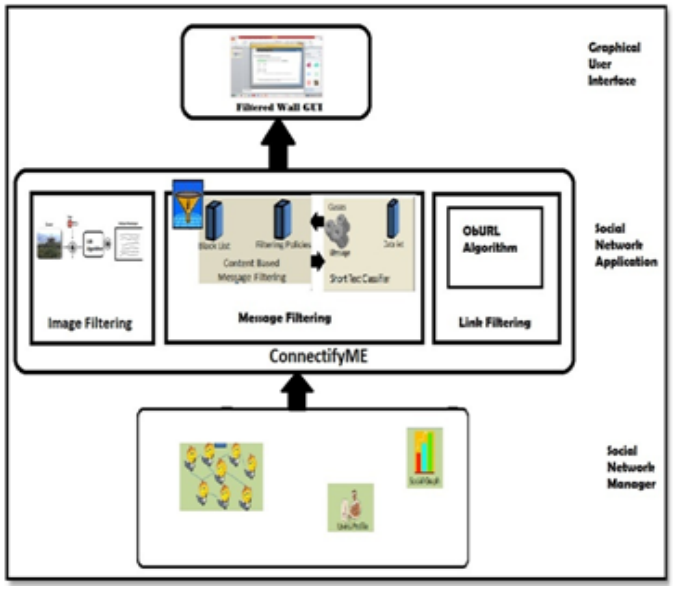

Figure 2: Block diagram of Filtering of Unwanted Message, Images and Phish Links on OSN.

A) Social Network Manager : The initial layer is Social Network Manager layer provides the essential OSN functionalities (i.e. profile and relationship administration). It also maintains al l the data regarding to the user profile. After administrating all users data will provide for second layer for applying Filtering Patterns (FPs) and Black lists(BL).

B) Social Network Application: In second layer Content Based Message Filtering (CMBF) and Short Text Classifier is composed. Also we are detecting phishing links and filtering images posted on user walls in this layer. This is very important layer for the message, images and link categorization. Also Black list is maintained for the user who sends frequently bad words in message. Links are filtered and the user the alerted if phishing link detected. Images are scanned and if found hidden messages are displayed.

C) Filtered Wall: Third layer provides Graphical User Interface to the user who wants to post his messages as a input and filtered wall is provided. In this layer Filtering Rules (FR) are used to filter the unwanted messages and provide Black list (BL) for the user who are temporally prevented to publish messages on user's wall. In this block diagram we are demonstrating the overall flow of the project implementation idea. Sender is the one who post messages/links or both on the user wall, for that sender should be friend of user. Before posting the post on the user wall, system will check if the user is blocked user or not. If it is the blocked user then the messages, image or links will be discarded and would not reach to the user wall, if it is not a blocked user, the filtering criteria will be applied on the message, images or links. Messages or post has to pass through Short Text Classifier and Content Based Message Filtering. In Short Text Classifier separates the message, images and links. The message will be classified as Neutral and Non-neutral according to the stored dataset. Non-neutral messages will be further filtered for Content Based Message Filtering to show the behavior and relationship between the user and further the sender from where the message arrives is blocked for a particular period of time. If the messages is neutral then it is posted on the user wall. The post contains a link it is processed by Link Guard Algorithm for checking if the link is phishing one or not. If the link found to be phishing then the user is alerted. The images are filter to know whether it is steganography images or not. If the image contains hidden messages then it is displayed to the user. Thus we have implemented a system which provides a Filtered Wall to the OSN user which filters the Messages, Links and Images.

V. UML DIAGRAMS

a) Use Case

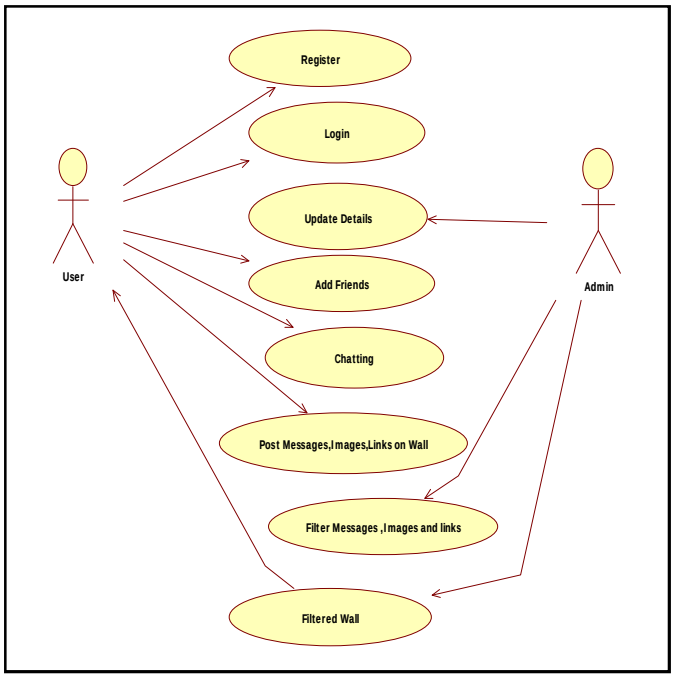

Figure 3: Use Case

The above diagram shows Use Case Diagram which defines the functionality of the system. It shows the Actors, functions and their interfaces.

b) Sequence Diagram

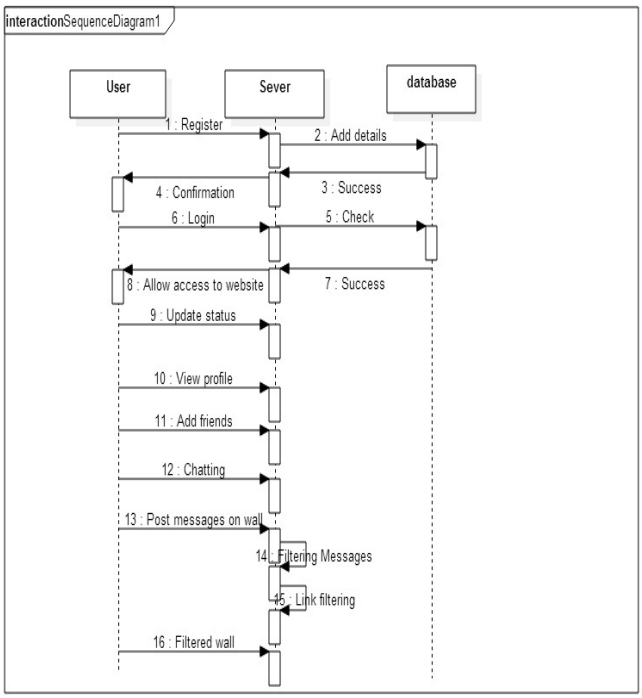

Figure 4: Sequence Diagram

Above sequence diagram describes the sequential flow of tasks of the system. It shows which task to perform in stepwise manner. It is also used to define the time constraints of the system.

c) Activity Diagram

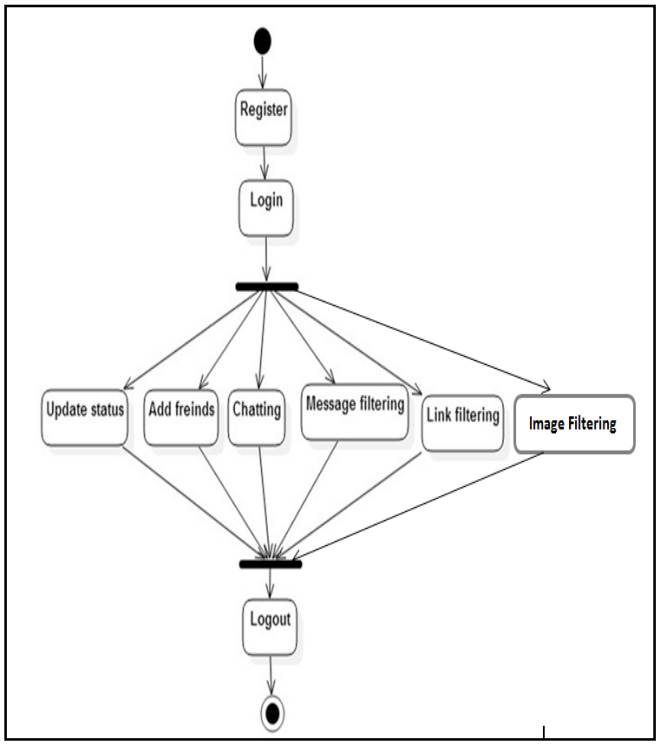

Figure 5: Activity Diagram

Above diagram shows the Activity Diagram which shows the actions and the data flow in them. It is similar to flowchart diagram which helps in implementing the system.

VI. FUTURE SCOPE

We can enhance this system by filtering audio and video files. We can even implement it as a web plugin which will be used as a tool for providing all the functionalities to different social networking sites and not for the specified one. In image filtering we can enhance the method by combining different algorithm used in image decrypting as message can be encrypted in images using any form of algorithm.

VII. CONCLUSION

We have implemented a system to filter undesired messages, images and links from OSN walls. We do consider that such a tool should propose expectation assessment based on users procedures, performances, and reputation in OSN, which might involve enhancing OSN with assessment methods. This tool helps in identifying hidden messages and displaying them. Though, the propose of these assessment based tools is difficult by several concerns, like the suggestions an assessment system might have on users' confidentiality and/or the restrictions on what it is possible to audit in present OSNs. However, we would like to remark that the system implemented represents just the core set of functionalities needed to provide a sophisticated tool for OSN message, image and link filtering. Thus, we provide a system that helps in reliable, efficient and secure use of OSN.

REFERENCES

[1] © 2014, IJARCSSE All Rights Reserved, Page | 33 Volume 4, Issue 2,February 2014 ISSN: 2277 128X "International Journal of Advanced Research in Computer Science and Software Engineering " Research Paper Available online at: www.ijarcsse.com

[2] "Anti-Phishing Technique to Detect URL Obfuscation "Jigar Rathod, Prof. Debalina Nandy M.Tech (CE) Researcher Scholar, RK University, India. Dept. Of Computer Engineering, RK University, India.

[3] International Journal of Communication Network Security, ISSN: 2231 – 1882, Volume-2, Issue-2, 2013 9 "Intelligent Phishing Website Detection And Prevention System" M.MADHURI 1, K.YESESWINI 2, U. VIDYA SAGAR3 1,2 B.TECH[CSE], SJCET, Yemmiganur. Asst. Professor, CSE Dept. SJCET, Yemmiganur, A P

[4] "A System to Filter Unwanted Messages from OSN User Walls" Marco Vanetti, Elisabeth Binaghi, Elena Ferrari, Barbara Carminati, Moreno Carullo Department of Computer Science and Communication University of Insubria 21100 Varese, Italy

[5] M. Chau and H. Chen, "A machine learning approach to web page filtering using content and structure analysis", Decision Support Systems, 2008

[6] M. Vanetti, E. Binaghi, B. Carminati, M. Carullo, and E. Ferrari, "Content-based filtering in on-line social networks," in Proceedings of ECML/PKDD Workshop on Privacy and Security issues in Data Mining and Machine Learning(PSDML 2010), 2010

[7] F. Sebastiani, "Machine learning in automated text categorization," ACM Computing Surveys, 2002

[8] Google Search Engine http://google.co.in