MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

NEW CLASSIFICATION AND FILTERING TECHNIQUE FOR SPAM MESSAGE OF ONLINE SOCIAL NETWORK (OSN)

Ganesh Waghmode, Akash Patil, Balaji Bahirwal, Akashy Thakare, Prof. Yogesh Thorat
DR. D.Y.Patil School of Engg. Lohegaon, pune.
Savitaribai Phule Pune University

Abstract: *Now a days we are going to update our status regularly on the social network sites like Facebook, twitter, etc. We can chat with our friends through these sites. The important problem of today's OSN is that it could not provide to the user to restrict the some messages, link, and images from the user. And also by using today's OSN sites we cannot control the unwanted messages. So in this paper we provide a way to user can restrict the messages, image, link which are unwanted are posted by their friends on the wall. We are going to use here flexible rule based system, that grant users to customize their filtering criteria to be applied to their walls and using a Link Guard Algorithm, OCR model for image filtering with algorithm.*

Keywords: *Filtered Wall, On-line Social Networks, Short text classifier, Machine Learning*

1. INTRODUCTION

Online Social Networks (OSNs) are today one of the greatest popular interactive medium for users to share, disseminate and communicate a considerable amount of human life information. Continuous and daily communications imply the sharing of several types of content, including free text, audio images and video data. The Facebook have stated that statistics the average user creates 90 pieces of content per each month, whereas more than 30 billion pieces of content (notes, web links, photo albums, blog posts, news stories, etc.) are shared per each month. Dynamic and huge character of these data creates the basis for the enrollment of web content mining strategies aimed to automatically discover useful information dormant within the data.

2. PROPOSED SYSTEM

The aim of proposed system is mainly to provide users a filtering mechanism to escape their walls overwhelmed by useless data. Due to the fact that in FACEBOOKs there is the possibility of posting or commenting other posts on distinct public/private areas. The information filtering can therefore be used to give the users the ability to automatically control the messages, links and images written on their own walls, by filtering out unwanted messages. We have invented the system to filter unwanted messages, images from FACEBOOK user wall. The images posted on the FACEBOOK wall which may contain very important information hidden in it, which leads to radical activities. For filtering the images we provide a OCR mechanism

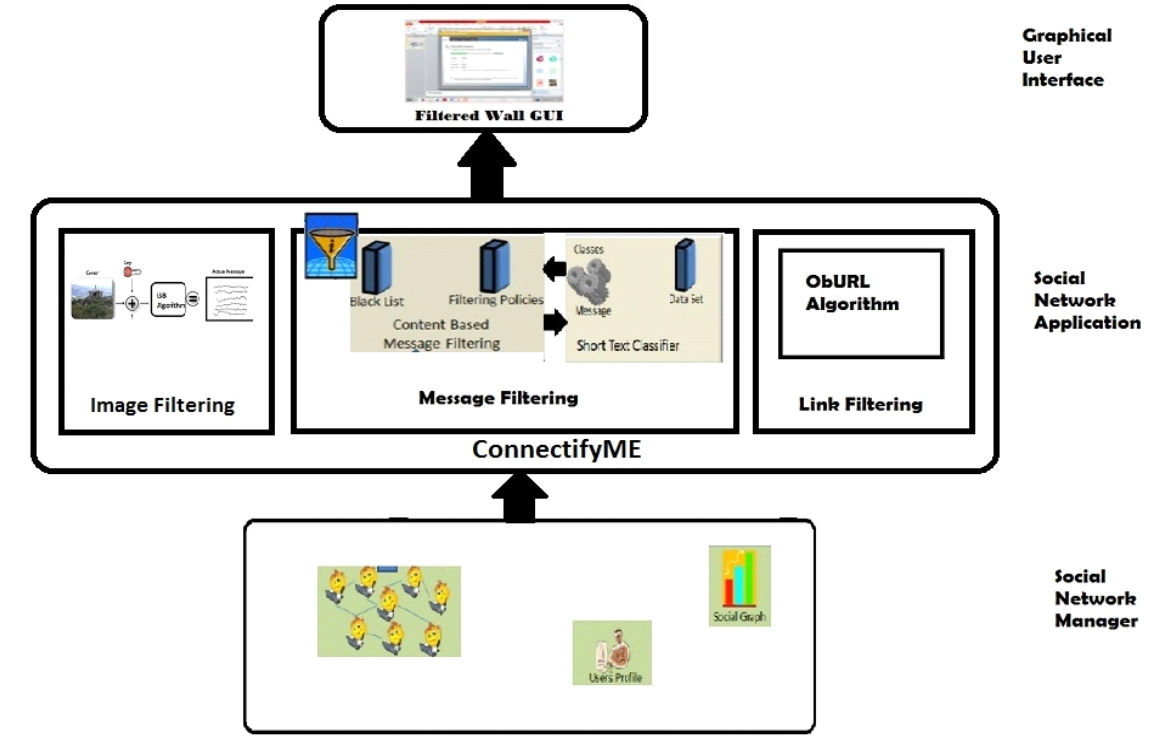

Fig1.architecture of OSN

A. Social Network Manager (SNM)

The basic layer is Social Network Manager Layer that provides the essential FACEBOOK functionalities (i.e., profile and relationship administration).It also maintains all the data related to the user profile. After managing and administrating all users data will provide for second layer for applying Filtering Patterns (FPs) and Black lists (BL).

B. Social Network Application (SNA)

In second layer is Content Based Message Filtering and Short Text Classifier is composed. Also we are identifying phishing links and filtering images posted on user walls in this layer. This is very vital layer for the message, images and link categorization. Also Black list is maintained for the user who sends again and again bad words in message. Links are filtered

and the user the alerted if phishing link detected. The images are scanned and if found the hidden messages are displayed.

C. Graphical User Interface (GUI)

The third layer provides GUI to the user who wants to send his messages as a input and filtered wall is provided. In this layer FR (Filtering Rules) are used to filter the unwanted messages and provide Black list for the user that 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.

3. RELATED WORK

3.1 FACEBOOK Wall

Online Social Networking is the application associated with the email address of the user. [3] contains no of functionality of chatting, posting messages, update status, adding friends and many more. Some of the examples are Facebook wall, Twitter etc.

3.2 Message Filtering

In [4] Marco Vanetti, Elisabetta Binaghi, Elena Ferrari have said that 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 activities are called filters and are specified through filtering rules. The filtering does not mean merely refusing messages or sorting them to folders, but it includes other actions such as automatic replies, notifications, forwarding the message to a different email address, etc.

3.3 Phishing

To study we refer the paper of Juan Chen and Chuanxiong Guo have presented [5] The term phishing is general term for the creation and use by criminals of emails and websites designed to look like they come from real, well-known and trusted businesses, financial institutions and government agencies–in an attempt to collect personal, financial sensitive information.

3.4 Image Spam Filtering

In IEEE, VOL. 26, NO. 1, JANUARY 2014, Improving Image Spam Filtering Using Image Text Features [6]**.** This papers show that how to detect the spam and ham on edited images. And now days Differentiation of Spam content from Ham content is an important consideration for maximum people. From that we helps to detect unwanted information.

4. COMPARISON

The existing system is same as the face book there is no phasing link and image filtering on OSN wall. To overcome that we proposed our system we use different algorithms for message filtering, link phishing and image filtering. In existing system there is no any method for message filtering, link phishing and image filtering. By using this system user can block the unwanted messages. User can identify the link phishing and user can also filter the images.

5. ALGORITHM

5.1 Link Guard Algorithm

1. Get the hyperlink for verification.
2. Extract the hypertext and anchor text. Check that both are same or not if not then alert the user.
3. If the hyperlink contains any input address, then check the IP Blacklist and IP White list. If IP address found in Blacklist then alert the user and if IP address found in White list then user is safe.
4. If the hyperlink is an encoded one, then the Phish Link detection algorithm will detect it, decode it and then will inform the user.
5. If the hyperlink is shortened then alert the user. Check the domain name of URL in White list and Blacklist and then alert the user respectively.

5.2 Message Filtering Algorithm

Input – (A, M, U, FP)

Output – (MT, BL)

Where A- System User

U – User posting message on A

M- Message posted on user wall A by U

FP – List of filter patterns of user A

MT – Message Type i.e. good or unwanted

BS - Blacklist

SentenceList () ←SentenceTokeniser (StopWordRemoval (M))

For each sentence in SentenceList ()

{ Intposcount=0, negcount=0;

For each filterpattern in FP {

```
        If (sentence.contains (filterpattern))
      SetmessageType ("Unwanted");
            Negcount++;
        Else
            SetmessageType ("Good");
            Poscount++;
       }
}
If (poscount>negcount) {
        AddToBlackList (M)
}
```

5.3 Phish Link Algorithm

1. Get the hyperlink for verification.
2. Extract the Visual Link and Actual Link. Check that both are same or not if not then alert the user.
3. If the hyperlink contains any input address, then check the IP Blacklist and IP Whitelist. If IP address found in Blacklist then alert the user and if IP address found in Whitelist then user is safe.
4. If the hyperlink is an encoded one, then the Ob URL detection algorithm will detect it, decode it and then will inform the user.
5. If the hyperlink is shortened then alert the user.
6. Check the domain name of URL in Whitelist and Blacklist and then alert the user respectively.

5.4 Naive Bayes algorithm steps (image filtering)

- Processing of training dataset
- Find out the conditional probabilities of each feature on those images.
- Find out the prior probability of spam and ham images
- Get the new image for classification
- Extract feature of this image
- Use the conditional probabilities and prior probability to calculate the probability of image to classify it in spam and ham.
- If image having higher probability in spam then classify it as spam or else in ham

6. ACKNOWLEDGMENT

We would like to thank Dr. D.Y.Patil School of Engg. for providing us with all the required amenities. We would thank our guide Prof. Yogesh Thorat sir for providing us help and guidance we needed. We are also thanks to Prof. S.S. Das, Head of Computer Engg. Department, DYPSOE, Lohegaon, for their indispensable support, suggestions and motivation.

7. CONCLUSION

We have implemented a system that filters unwanted messages, images and links from FACEBOOK walls. We do consider that such a tool should propose expectation assessment based on users procedures, performances, and reputation in FACEBOOK, which might involve enhancing FACEBOOK 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 FACEBOOKs. However, we would like to remark that the system implemented represents just the core set of functionalities needed to provide a tool for FACEBOOK message, image and link filtering. Thus, we provide a system that helps in reliable, efficient and secure use of FACEBOOK.

REFERENCES

[1] IJARCSSE All Rights Reserved, Page | 33 Volume 4, Issue 2, and February 2014ISSN: 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"JigarRathod, Prof. DebalinaNandyM.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 FACEBOOK User Walls" Marco Vanetti, Elisabetta Binaghi, Elena Ferrari, Barbara Carminative, Moreno Carullo Department of Computer Science and Communication University of Insubria 21100 Varese, Italy.

[5] Juan Chen and Chuanxiong Guo "Online Detection and prevention of phishing attacks" ©2006 IEEE

[6] IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 1, JANUARY 2014,Improving Image Spam Filtering Using Image Text Features.