FILTERING OF UNWANTED MESSAGES, IMAGES AND PHISH LINKS ON OSN WALL

M. G. Devikar[1], Tejashree Dhole[2], Neha Hivarkar[3], Vaishali Bhagat[4], Varsha Bhosale[5]

[1]Professor, Computer, MESCOE, Maharashtra, India
[2]Student, Computer, MESCOE, Maharashtra, India
[3]Student, Computer, MESCOE, Maharashtra, India
[4]Student, Computer, MESCOE, Maharashtra, India
[5]Student, Computer, MESCOE, Maharashtra, India

Abstract

OSN being an important media of communications and building relationship on Internet. It is generally being influenced by many factors some of those are, OSN user has to deal with unwanted post or messages on their walls which are vulgar or of no meaning. It may also contains political, casteism related rumors which may cause riots in the social media. Links which are been posted on wall may be phishing and may mislead the user and images spreading on OSN wall may contain hidden messages which are carried out by some terrorist groups. To overcome the above problems a new proposed system "Filtering of Unwanted Messages, Images and Phish Links on OSN wall" an online application is proposed. The message filtering technology helps the OSN wall user to avoid from getting unwanted message from all the users on social networks. The phishing link detection technology is use to secure the OSN user from getting phishing links and avoid from further attacks. The system also provides filtering of images through steganography , that is retrieving the hidden messages from the images.

Keywords: *OSN, Filtered Messages and Images, Steganography, Phish Links.*

---***---

1. INTRODUCTION

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 OSNs 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 OSN user walls. The images posted on the OSN 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 OSN 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.

2. EXISTING SYSTEM

According to literature survey on OSN that has been provided so far. Indeed, today OSNs provide very little support to prevent unwanted messages on users wall. For example, Facebook allows users to state who is allowed to insert messages in their walls (i.e., friends, friends of friends, or defined groups of friends). However, no filtering based preferences are supported and therefore it is not possible to prevent undesired messages, such as political or vulgar ones, no matter of the user who posts them. Also today's system does not provide any filtering of images which may contain secret transfer of data and messages in a chaos of OSN user.OSN been used very vastly it is a target by many terrorist activities, hackers which may mislead the user and cause harm to their security.

2.1 Limitations

- User cannot avoid unwanted messages delivered on OSN walls.
- Phishing link are not detected leading user redirect to phishing site that may cause stealing of user's credential data.
- Short-text classification does not provide sufficient word occurrences.
- Images are not filtered for steganography so far.

3. LITERATURE SURVEY

In this chapter there search work is been studied, it contains the learning aspects related to the system defined in problem description. All the related information, papers are searched and knowledge about the topic is elaborated below.

3.1 Background of the Project

Online Social Networking wall 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.

Message Filtering is, When a message is delivered to a local user of Mail Server, it is stored in the INBOX folder. In WebMail, 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 criminal so fe-mails and web sites 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 user names 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.

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. The key idea of the implemented system is the support for content- based user preferences, this is possible due to the use of a Machine Learning text categorization procedure able to automatically assign with each message. We believe that the implemented strategy is a key service for social networking user in today's time where social networks users that have little control on the messages, images and links displayed on their walls. For instance, it is also possible to prevent political or vulgar messages spreading which are causing harm to the social media.

By means of the implemented system, a user can specify what contents should not be displayed on his/her wall, by specifying a set of filtering patterns. Filtering rules are very flexible in terms of the filtering requirements they can support, in that they allow to specify filtering conditions based on user profiles, user relationships. In addition, the system provides the support for user- defined blacklist management, that is, list of users that are temporarily prevented to post messages on a user wall. Images on the wall are also filtered if contains any hidden text that is spreading through the images on OSN wall, which give an approach of identifying the terrorist activities. It also filters the links posted on the wall to help user to identify the phishing activities and to prevent them from such links by giving alert.

3.2 Domain of the Study

The project basically comes under information security domain. The key concept of information security in project is that the system prevents the OSN users from fraudulent attackers. Even the messages and images which are not vital for a user are filtered. In addition, the system provides the support for phish link detection that are prevent users from attacks.

3.2 Motivation of the project

As the growing use of Social Networking sites in day to day life, it has become necessary to secure the Online Social Networking and make it more reliable to the user to use it. Our intention to develop this system is secure the OSN users from phishing links and the steganographical images that may spread unnecessary information through the OSN wall.

Also our purpose is to provide the user with the user defined patterns which the user can give to filter OSN wall according to user requirements. This will make the use of OSN for the users more secure, reliable and under control of the user. The aim of the present work is to propose and experimentally evaluate an automated system, called Filtered Wall (FW), able to filter out unwanted messages, images from social network user walls.

4. PROPOSED SYSTEM

We have implemented the system called ConnectifyMe, which contains all the features of Online Social Networking such as Register, Login, Upload Image, Upload post, Friend request etc. In this system we are providing the user with user defined filtering patterns which are given by the user itself to the system and according the user wall is filtered, the sender sending such message are blacklisted automatically by the system and if it exceeds more the three times by the same user he/she is blocked. ConnectifyMe also provides filtering of images which contains hidden text in it, such images are filtered and the text is displayed. The system also provides filtering the phishing links posted on the user walls, alerting the user to proceed or not with the link if found phishing, so to prevent users credentials information from leaking.

The aim of the present work is experimentally evaluate an automated system, called ConnectifyMe, able to filter unwanted messages, images and phish links from OSN user walls. Thus we are providing a solution as ConnectifyMe to make the use of OSN wall more efficient, reliable and secure to the user, through which user can have control of what should be displayed on its own wall.

4.1 Objectives

1. Filtering unwanted information from OSN wall as per user requirement.
2. Alert user from phishing links and sites.
3. Images are scanned to identify whether it contains any text hidden in it, and thus the image is discarded.
4. Making OSN more reliable, secure, trustworthy and comfortable for the user.

5. IMPORTANT MODULES & ALGORITHMS

There are three important modules in this system:

5.1 Message Filtering

In this module, the unwanted messages are filtered. The other users that can send vulgar message to an OSN user is temporarily blocked by the OSN user. If the user sends vulgar messages that match the filtering pattern specified by the OSN user more than a specified threshold value than that user is unfriend permanently.

5.1.1 Filtering Rules

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 write sit. 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. 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. The same message on OSNs may have different meanings and relevance based on who write sit. It is necessary to apply constraints on messages. Constraints can be selected on several different criteria's. User can state what contents should be blocked or displayed on filtered wall by means of Filtering rules. Filtering rules are specified on the basis of user profile as well as user social relationship. FR is dependent on following factors,

1. Author
2. Creator Spec
3. Content Spec
4. Action

An authorize person who defines the rules. CreatorSpec denotes the set of OSN user and ContentSpec is a Boolean expression defined on content. Action denotes the action to be performed by the system on the messages matching contentSpec and created by users identified by creatorSpec.

5.2 Image Filtering

In this module, the images are filtered. Those images that contain vulgar names are filtered and that particular image is not rendered on the OSN wall of the user that uses this facility.

Algorithm for Encoding the Image

1. Convert the data from decimal to binary
2. Read Cover Image
3. Convert the Cover Image from decimal to binary.
4. Break the byte to be hidden into bits.
5. Take first 8 byte of original data from the Cover Image.
6. Replace the least significant bit by one bit of the data to be hidden.

Algorithm for decoding the Image:

1. Convert the data from decimal to binary.
2. Read cover image
3. Convert the cover image from decimal to binary.
4. Break the byte to be hidden into bits.
5. Take first 8 byte of original data from the cover image.
6. Replace LSB2 by one bit of the data to be hidden.

5.3 Phish Link

1. Get the hyperlink for verification.
2. Extract the hyper text 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 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 ObURL 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.

6. SYSTEM IMPLEMENTATION

The system implementation contains the following modules that are essential to build the system,

6.1 Modules

1. User Registration (Sign In / Sign Up)
2. Adding/Inviting Friends
3. Chatting/Messaging
4. Post on User Wall
5. Filtering patterns
6. Image filtering through steganography.
7. Phishing prevention on links posted on user walls
8. Blacklists.

7. SYSTEM ARCHITECTURE

Three tier architecture is used in OSN services. These three layers are,
1. Social Network Manager (SNM)
2. Social Network Application (SNA)
3. Filtered Wall (FW)

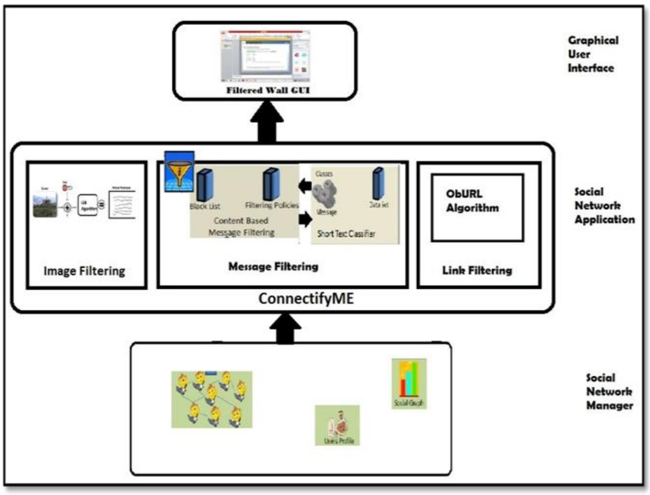

Fig -1: System architecture of Filtering of Unwanted Messages, Images and Phish Links on OSN Wall.

7.1 Social Network Manager (SNM)

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

7.2 Social Network Application (SNA)

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.

7.3 Graphical User Interface (GUI)

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.

8. TESTING

The testing was performed to degrade the software failures and to increase the fault tolerance capability of the system. It was taken into consideration that if there are any flaws in the software that were uncovered in the testing process, the logical errors were detected and corrected.

The various testing types that were carried out for checking the accuracy of this system are: unit testing, integration testing, black box and white box testing, validation testing.

The testing period for this system was carried out for 20 days after the system was implemented. In the initial phase, unit testing was carried out for modules such as filtering rules, phish link detection and steganographic images. The the integration testing was done on all the modules by running the project on more than one system. Accordingly, the results were noted and the improvements were made. As the system got habituated to fault tolerance the number of systems were increased. The below table predicts the results of testing carried out:

Table -1: Test Case for Accuracy of the System for Fault Tolerance:-

No. of Systems used	Images	Messages	Phish Links	Fault Tolerance	Accuracy
1	2	10	5	Messages-10 Links-5 Images-2	99%
5	5	10	15	Messages-8 Links-13 Images-3	80%
10	15	150	95	Messages- 8 Links-13 Images-11	89.61%.
Total Accuracy for each	72.72 %	88.23%	93.91 %		

System Accuracy = 89.25%

The above table shows the results for the testing carried out on this system. In an heterogeneous environment the use of this system is considerable. It can tolerate more faults on a network. The table shows that when the tendency of the system is increased i.e number of system is increased by 10 then the overall accuracy of the system is also increased by 83.61 %, thus increasing its fault tolerance capability.

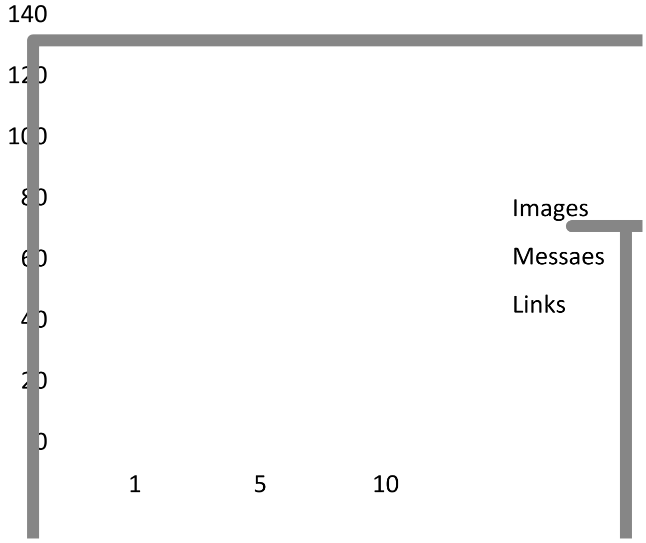

Chart -1: Resulting graph derived from Table.1

The above graph shows that when the number of system is increased in a network where the use of this system is highly recommended there it puts the maximum accuracy and through put. The horizontal axis in the chart shows the number of systems and the vertical lines in the chart shows the fault tolerance number.

9. FUTURE WORK

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.

10. 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.

ACKNOWLEDGEMENTS

We take this opportunity to express our profound gratitude and deep regards to our respected Pricipal Dr. A. A. Keste, H.O.D. Prof. N. F. Shaikh and our Project Guide Prof. M. G. Devikar for their guidance, monitoring and constant encouragement throughout the course of this thesis.

REFERENCES

[1]. © 2014, IJARCSSE All Rights Reserved, Page | 33 Volume 4, Issue 2,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 "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 E-mail:madhurimitai01@gmail.com, yeshukandagaddala@gmail.com, engg.sagar@gmail.com

[4]. "A System to Filter Unwanted Messages from OSN User Walls". Marco Vanetti, ElisabettaBinaghi, Elena Ferrari, Barbara Carminati, Moreno Carullo Department of Computer Science and Communication University of Insubria 21100 Varese, Italy. E-mail: moreno.carullog@uninsubria.it

[5]. "Towards Detecting Anomalous User Behaviour in Online Social Networks" Bismal Vishwanath, M.Ahmad Bashir, Mark Crovella, Saikat Guha.

[6]. A. Adomavicius, G.andTuzhilin, " Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions ", IEEE Transaction on Knowledge and Data Engineering,2005.

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

[8]. R. J. Mooney and L. Roy, " Content-based book recommending using learning for text categorization ", in Proceedings of the Fifth ACM Conference on Digital Libraries. New York: ACM Press, 2000.

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

[10]. 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.

[11]. N. J. Belkin and W. B. Croft, "Information filtering and information retrieval: Two sides of the same coin ", Communications of the ACM,1992.

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