FILTERING OF IMAGES, PHISH LINKS AND UNSOLICITED CONTENT FROM ONLINE SOCIAL NETWORK USER WALL

Martand Ratnam[1], Dr Santosh Kumar Shukla[2], Atul Kumar Singh[3],

Kaushal Kumar[4], Dr Shwetav Sharad[5], Bharti Sharma[6], Ankit Tomer[7]

1(Computer Science and Engineering, AKTU Lucknow Email:martandratnam@gmail.com)

2(Computer Science and Engineering, BBDEC Lucknow Email:santosh.knmiet@gmail.com)

3(Computer Science and Engineering, BBDIT Ghaziabad Email:ksgatul@gmail.com)

4 (Computer Science and Engineering, RKGIT Ghaziabad Email:kaushal581@gmail.com)

5 (Computer Science and Engineering, BBDIT Ghaziabad Email:shwetav.sharad@gmail.com)

6 (Computer Science and Engineering, NIET Greater Noida Email:bhartisharma0811@gmail.com)

7 (Computer Science and Engineering, JMS college Hapur Email:ankittomer02@gmail.com)

Abstract

Online Social Network being a significant media of interchanges and establishing relationships online. It is for the most part being affected by numerous elements a portion of those are, OSN client needs to manage unwanted posts or irrelevant, offensive statements on their walls. It might likewise contains casteism and political related bits of hearsay which might cause riots in the virtual entertainment. The client may be misdirected by posts on the wall that are phishing links, and the photographs that are spreading on the OSN wall might include secret messages. that are the work of some fear-mongering groups. To beat the above issues another proposed framework " Separation of Phish Links, Images, and Unwanted Messages on OSN Wall " a web-based application is suggested. The message separating innovation assists the OSN with walling client to keep away from receiving undesirable message from every one of the clients on informal communities. The phishing join identification innovation is use to get the OSN client from getting phishing joins and stay away from additional assaults. The framework likewise gives separating of pictures through steganography , that is recovering the concealed messages from the pictures.

Keywords: *Phish Links ,Filtered Images and Messages, Steganography, Online Social Network (OSN)*

***

1. INTRODUCTION

The point of this framework is chiefly to give clients a separating system to stay away from their walls overpowered by futile information. Due to the the potential to submit or remark on various postings on a certain public /confidential locations in OSNs. By filtering out unwanted communications, data separation can be used to give users the ability to organically govern the messages written on their own walls. We created a robotized framework called ConnectifyMe that is prepared to transmit unwanted messages and images from OSN client walls. the images uploaded on the OSN's wall that might have important information hidden in them and cause oppressive exercises based on fear. We use a steganography tool to filter the images, which interprets the hidden data and makes it more secure.

There are potential outcomes of phishing joins being posted on the OSN walls, accordingly to caution the client about the phishing join, framework is utilizing an enemy of phishing calculation called obURL, which has six unique moves toward channel the connection and alarm the client in the event that it is identified to phishing site.

2. EXISTING SYSTEM

Based on the literature review on OSN presented up to this point. Of course, OSNs presently provide very little assistance in preventing unwanted messages from appearing on users' walls Facebook, for instance, allows users to choose who may post messages on their walls (i.e., friends, friends of friends, or specially arranged groups of friends.). However, because no separation-based options are offered, it is challenging to prevent undesirable communications, such as political or revolting ones, independent of the client who submits them. Likewise the present framework doesn't give any separating of pictures which might enclose a secret exchange of information and messages in a tumult of Online Social Network user. Online Social Network been utilized boundlessly it is an objective by numerous psychological militant exercises, programmers which might misdirect the client and really hurt their security.

2.1 Limitations

- User cannot avoid unwanted messages delivered on OSN walls.
- When phishing links are not recognised, users are sent to phishing sites where their credentials may be stolen.

Word occurrences from short-text categorization are insufficient.

Steganography detection has not yet been applied to images.

3. LITERATURE SURVEY

This section takes into account search work, it contains the learning perspectives connected with the framework characterized in issue portrayal. All the connected data, papers are looked and information about the point is expounded beneath.

3.1 The Project's History

Online Social Networking (OSN) Wall is the programme connected to the user's email account. It contains different functionality of chatting, posting messages, update status, adding friends and many more. As for examples Facebook wall, Twitter etc.

When a message is sent to a Mail Server client in the immediate area, it is stored in the INBOX envelope. Every client can specify a number of actions to be taken on all incoming messages in WebMail, along with the conditions surrounding them. These activities are called channels and are indicated through separating rules. Sifting doesn't mean only declining email messages or arranging them to envelopes, yet it incorporates different activities, for example, notices, programmed answers, sending the message to an alternate email address, and so on.

The practise of criminals creating and using e-mails, websites, and other communications that appear to be from well-known, reputable, and trustworthy companies, financial institutions, or governmental organisations in an effort to get sensitive personal or financial data is known as "phishing." These criminals can access people's computers or bank accounts by fooling them into handing over their personal information, such as user names and passwords, or into unwittingly putting dangerous software onto their machines.

The system that offers a safe solution to the OSN wall and its associated issues is called ConnectifyMe. The technology is capable of removing undesired posts, photos, and links from user walls on social networks. The support for content-based client preferences is the key concept of the implemented framework; this is made possible by the use of a Machine Learning message order strategy that is prepared to distribute with each message in turn. We accept that the executed technique is a critical help for person to person communication client in the present time where informal organizations clients that have little control on the messages, pictures and connections showed on their walls. For example, it is additionally conceivable to forestall political or indecent messages spreading which are hurting the online entertainment.

By providing a number of filtering designs, the customer may use the finished framework to decide what should and should not be displayed on his or her wall. Sifting rules allow for the determination of sifting conditions based on client profiles and client relationships, making them incredibly flexible in regard to the separate requirements they may support. Additionally, the framework provides assistance for client-characterized executive boycott, that is, a list of clients who are momentarily prevented from posting remarks on a client wall. Additionally, if any hidden text is present among the photographs on the OSN wall, those

images are isolated. which give a methodology of distinguishing the fear based oppressor exercises. It likewise channels the connections presented on the wall on assist client with recognizing the phishing exercises and should warn people of such links in order to prevent them.

3.2 Study's Domain

The project largely fits within the information security area. The main idea behind the project's information security is that the system protects OSN users against malicious attacks. Even texts and graphics that the user does not need are screened. Additionally, the technology supports the identification of phishing links, protecting users from assaults.

3.3 Purpose of the project

It is now crucial to study Online Social Networking (OSN) and make it easier for the user to utilise it due to the growing usage of social networking sites (SNS) in everyday life. Our intention in supporting this framework is to protect OSN clients against steganographic images and phishing joins that might disseminate useless data across the OSN wall.

Additionally our motivation is to furnish the client with the client characterized designs which the client can provide for channel OSN wall as per client necessities. This will utilize OSN for the clients safer, dependable and taken care of the client. The purpose of the current effort is to suggest and provisionally evaluate Filtered Wall (FW), a robotized framework ready to sift through unwanted messages and images from unofficial community client walls.

4. SUGGESTED SYSTEM

We have put the ConnectifyMe framework in place. which includes all of the key features of online social networking, including register, login, upload image, upload post, friend request, and more. In this framework we are furnishing the client with client characterized sifting designs which are given by the actual client to the framework and agreeing the client wall is separated, the source sending such message are boycotted naturally by the framework and assuming it surpasses more the multiple times by a similar client he/she is impeded. ConnectifyMe likewise gives sifting of pictures which contains stowed away text in it, such pictures are separated and the text is shown. The framework likewise gives sifting the phishing joins posted on the client walls, making the client aware of continue or not with the connection whenever found phishing, so to keep clients certifications data from spilling.

The goal of the current study is to provisionally evaluate ConnectifyMe, a robotized framework prepared to channel unwanted messages, images, and phishing joins from OSN client walls. As a result, we are offering ConnectifyMe as a solution so that clients may use OSN Wall in a more productive, reliable, and secure manner and have control over what is displayed on their own Wall.

4.1 Goals

1. According to user needs, removing undesirable information from the OSN wall.
2. Warn the user of phishing websites and connections.
3. Images are checked to see whether there is any text buried inside them, and if there is, the image is discarded.
4. Improving OSN's dependability, security, credibility, and user-friendliness.

5 IMPORTANT MODULES & ALGORITHMS

This system contains three crucial modules:

5.1 Message Filtering

Unwanted communications are screened in this module. Other users that are able to send offensive messages to OSN members include

The OSN user has temporarily prohibited access. When a user exceeds a certain threshold for vulgar communications that meet the filtering pattern established by the OSN user, that user is permanently unfriended.

5.2 Filtering Rules

When expressing the language for FRs determination, we take into account three crucial urgent factors that ought to have an impact on a message separation choice. In OSNs, like in real life, the same message may be interpreted and relevant in multiple ways depending on where the compose sits. As a result, FRs should let clients impose restrictions on message producers. One of the most important criteria for selecting makers to whom a FR applies is placing restrictions on their profile's credits. Given the context of interpersonal organisation, decision-makers can also be identified by drawing on information from their social network. This suggests to state conditions on type, profundity and trust upsides of the relationship makers ought to be engaged with request to apply them the predefined rules. A similar message on OSNs might have various implications and importance in light of who compose sit. Applying imperatives on messages is essential. Several different criteria can be used to select imperatives. Through Filtering rules, the client may specify what things should be blocked from view or shown on the sifting wall. Sifting criteria are established based on client social relationships as well as client profiles. FR depends on the following things:

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

an authority figure who establishes rules. While ContentSpec is a Boolean expression that is provided on material, CreatorSpec refers to a group of OSN users.Action refers to the procedure that the system will follow when messages that fit the contentSpec and were produced by users indicated by the creatorSpec are received.

5.3 Image Filtering

The photos in this module have been filtered. Images with profane names are filtered, and the person who utilises this function will not see that specific image on their OSN wall.

Algorithm for Encoding the Image

1. Binary to decimal data conversion
2. View Cover Image

3. Binaryize the Cover Image by converting it from decimal.
4. Split the byte into bits so it may be concealed.
5. Extract the first 8 bytes of the cover image's original data.
6. Substitute one of the data's to-be-hidden bits for the least important bit.

Algorithm for decoding the Image:

1. Transform the binary data into decimal.
2. Read cover photo
3. Binaryize the cover picture by converting it from decimal.
4 Divide the concealed byte into bits.
5 Take the first 8 original bytes of the cover picture.
LSB2 should be replaced with one of the data's hidden bits.

5.4 Phish Link

1. For verification, get the hyperlink.
2. Remove the anchor text and hypertext. Verify whether the two are same; if not, notify the user.
3. Verify the IP Blacklist and IP Whitelist whether the hyperlink contains any input addresses. If an IP address is identified on a blacklist, the user is warned; otherwise, the user is safe.
4. The ObURL detection method will identify an encoded hyperlink, then notify the user after decoding it.
5. Inform the user whether the hyperlink has been shortened.
6. Verify the URL's domain name in the Blacklist and Whitelist, and then notify the user, if appropriate.

6. IMPLEMENTATION OF A SYSTEM

The following modules are included in the system implementation and are necessary to construct 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

Online social networks have a three-tiered design. (OSN) services. These three layers are

1 Social Network Application (SNA)
2 Social Network Manager (SNM)
3 Graphical User Interface (GUI)

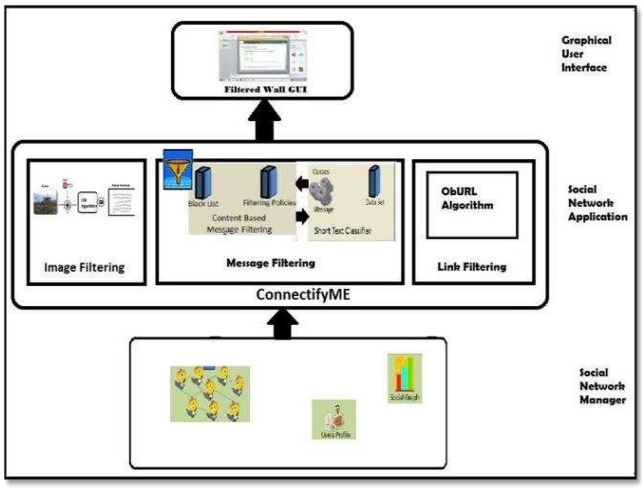

Fig -1: System architecture of Filtering of Phish Links, Images and Unwanted Messages on Online Social Network (OSN) Wall.

7.1 Social Network Manager (SNM)

The basic Social Network Manager level offers the necessary OSN functionality. (i.e., relationship and profile). It also keeps track of information about the people with whom you've interacted. Filtering rules and black lists will be applied to all user data sent to the second layer (BL).

7.2 Social Network Application (SNA)

The second layer is made up of Short Text Classifier (STC) and Content Based Message Filtering (CBMF). This level is crucial for categorising messages. Additionally, a black list (BL) is kept for foul language and users who submit it regularly.

7.3 Graphical User Interface (GUI)

An application with a Graphical User Interface (GUI) is used in the third layer by users who want to send their messages as input. Utilizing Filtering Rules (FR), this layer's additional primary duty is to screen undesired communications. Users who submit such messages are maintained on a Black List (BL) until the user removes them. Additionally, the GUI offers a filtered wall (FW) where users may publish and see the messages they want to see.

8. TESTING

Testing was done in order to corrupt the product disappointments and to expand the adaptation to non-critical failure ability of the framework. It was thought about that assuming if the product has

any flaws that the testing procedure revealed,the coherent mistakes were recognized and adjusted.

Black box testing , Integration testing, Unit testing , validation testing, and White box testing are some of the several testing kinds that were done to verify the accuracy of this system.

This framework underwent tested for a period of 20 days following its execution. In the underlying stage, unit testing was carried out for modules including steganographic pictures, phish connect recognition, and separation rules. By executing the task on many frameworks, the mix testing for each of the modules was completed. The results were appropriately acknowledged, and improvements were made. As the framework became more adept at adjusting to non-critical failure, the number of frameworks increased. The following table forecasts the outcomes of the testing that was done:

Table -1: Test Case for the System's Accuracy in 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 results of the testing done on this framework are displayed in the table above. This framework is extensively utilised in diverse environments. It can withstand greater criticism directed at a company. The table demonstrates that as the propensity of the framework increases, or as the number of frameworks increases by 10, so does the general exactness of the framework, increasing its capacity to adjust to internal failure by 83.61%.

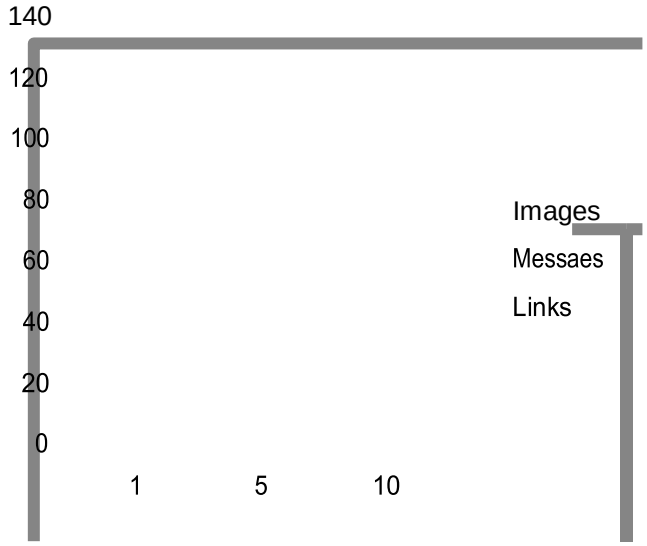

Chart -1: Graph produced as a result of Table 1.

The graphic above demonstrates that the best accuracy and throughput are produced when the amount of the framework is increased in an organisation where its use is strongly advocated. The diagram's level hub represents the number of frameworks, while the outline's rising lines represent the adaptation to non-critical failure rate.

9 CONCLUSION

We've put in place a method to remove undesirable connections, photos, and postings from Online Social Network (OSN) walls. We are adamant that such a tool should advise making an assessment of the hypothesis in light of client techniques, displays, and reputation in Online Social Network (OSN), which could need upgrading Online Social Network (OSN) with evaluation techniques. This tool assists in finding and displaying hidden messages. However, the notion of these assessment-based devices raises several concerns, such as the potential impact that an evaluation framework may have on clients' privacy and the scope of what can be audited in current OSNs. Notwithstanding, we might want to comment that the framework executed addresses simply the features in the centre were set up to provide OSN messages a complex tool, picture, and connection splitting. Hence, we give a framework that aides in dependable, effective and secure utilization of OSN.

10 UPCOMING WORK

We can improve this framework by sifting video and sound records. We could in fact carry out it as a web module which will be utilized as a device for giving every one of the functionalities to various person to person communication locales and not for the predetermined one. In picture separating we can upgrade the strategy by joining different calculation utilized in picture unscrambling as message can be scrambled in pictures utilizing any type of calculation.

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.