International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 12 4086 - 4090

Filtration in OSN for Personalized Message

Gaurav N. Gharte[1]
Student of BE Information Technology
BVCOE & RI, Nasik, India
University of Pune
ghartegaurav111@gmail.com

Bhuvaneshwari B. Ugale[2]
Student of BE Information Technology
BVCOE & RI, Nasik, India
University of Pune
bhumiugale@gmail.com

Bhagyashri B. Pagar[3]
Student of BE Information Technology
BVCOE & RI, Nasik, India
University of Pune
pagarbhagyashri92@gmail.com

Prof. Kavita S. Kumavat[4]
ME Computer Engineering
BVCOE & RI, Nasik, India
University of Pune
kavitakumavat26@gmail.com

Abstract **-** In recent year's online social network (OSN) is popularly increased day by day in the form of sharing, commenting, posting, tagging messages or other data. Today's condition about unwanted post or unwanted messages in social networking is very bad thing happens when peoples work on social networking then unwanted malicious data is post by any person on their wall. System provides a safety by providing the variety of filtering method for data. Also system gives security to user when someone is repeatedly post or share unwanted data. Reliability is provided by system to user by giving offline security that reduce user's efforts in always online to safe from unwanted data from OSN wall. For user provide the facility to create a blacklist (BL) which is for block a person for particular duration when he/she irritate from that person's vulgar messages. Whenever user sends a message or comment on another user wall against his/her wish then recipient user does him/her in blacklist. All this things also covered by Undo function and User can able to undo message. System include two sections that for both peoples in this way those who don't like unwanted or malicious data and those who want malicious data. Short text classification method is use for finding or filtering malicious data. Stemmer algorithm is use filtered data for word comparison and finding unnecessary data and stop word algorithm use for blocking unwanted words from user OSN wall.

Keywords- *Online Social Network, Blacklist, Machine Learning, Filtered Wall, Short Text Classifier.*

*****

I. INTRODUCTION

In recent years online social networking services become very popular among the users like Facebook. Social networks which use online service are allowed to user or peoples to join to other organization it may be business or other fields. Because of the popularity of these services and applications comes with the some problems of unwanted messages to user walls because of these problems user's daily activities in social networking is influenced. In recent years, online social networks have popular way to communicate with people's world widely. In that share, comment or post these things are mainly includes. There is large amount of data is shared or posted in the form of messages, comments etc. This thing contains wanted and unwanted data according to user needs. User's faces many problems because of OSN wall unwanted post by using message filtration method it can be easily removed in OSN for better communication. In system data classification method is used to avoid unwanted data. In this paper filtering methods can be different on data, this is happens due to the factors that in OSN there is possibility of posting or commenting other posts on some areas, known as general walls. Information filtering user can automatically manage the system that who will be writing a message on his /her OSN user wall. In facebook ask for permit to user when someone gets posted on his social wall but it is only ask about what type of person post on his/her wall. There is no precedence based functioning done malicious, vulgar messages are also taken as good content on user wall. That will pay a cost insult to user own on in front of world. This problem can be defeat in this system. In this system also provide a ability for user perspective to take decision what type of data should be user want to see as two sections data one is unfiltered wall (general wall) and other is filtered wall. Filtered wall shows user choice messages in the OSN of user wall and other hand side is used for all the messages are shown to user on their wall. This system also gives to user surety about fake accounts doesn't allow. That means it will be helpful in the perspective of user need.

This approach helps user to find known as well as unknown person in which he/she is interested in that field for making friends. Filtering technique is done automatically in the system when user online or offline in OSN. That means also a new feature added in that system to provide offline security. Text categorization techniques in machine learning are also used in system for allocating the short text based on the content automatically. Assured steps are included in this technique like short text classifier is first step, blacklists and filtering rules. Message filtration is done

ISSN: 2321-8169
4086 - 4090

automatically this is called filtered wall. Filtered wall is used for filter unwanted message.

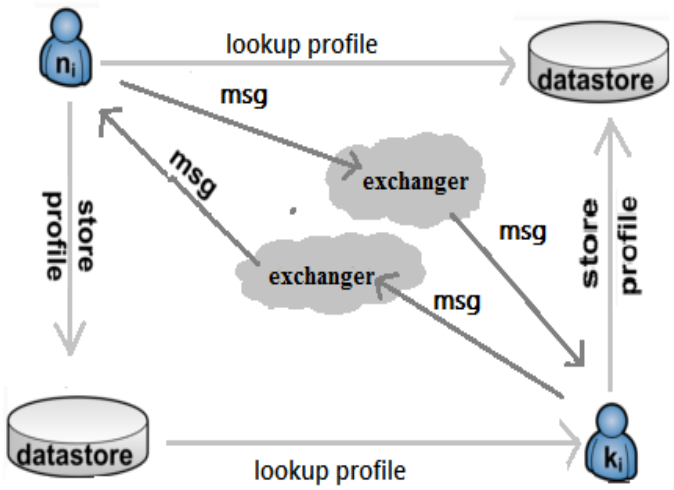

Figure 1: Message flow Architecture

Figure 1 shows the basic architecture of flow of message in social networking. It first involve searching or looking for profile and then the messages are exchange between two different users. Also the exchange messgae will be store in appropriate database.

II. LITERATURE SURVEY

Existing online social networking sites security problems are mostly occurs like fake accounts unidentified friend request are received by unknown peoples etc [5]. When user share or post anything on OSN between among users there must be follows the possible risk. There is no any ID provides for the user therefore one user can create more accounts with different names. This help to illegal event [2]. In current system content based filtration are not provided therefore there is impossible to prevent unwanted messages from user walls such as political, social etc contents and there is no need of who post that messages [10]. In some social networking site limitation to send friend request and create groups. Whenever notifications are receiving from other peoples that time they show in complex forms therefore that are difficult to see. No any filtration presented for post and share content therefore any known unknown person post on others walls. Social networking sites are usually used for daily communication over worldwide [1]. Therefore in system all weak point of existing system are defeat. The main factor of the system is to provide a security over a internet for user wall in OSN where filtering is done and rejects the unnecessary data or messages [2] [6]. Online security is provided to the user walls. The main ambition of system provides filtered wall and blacklisting to user walls. These two methods are essential in today's life because social networking sites are more popular approximately 30 billion contents are post in one month [11]. In system content based filtering and policy based filtering are use. In system arriving messages are firstly taken under algorithms then they are shown on user's wall [3][7]. For blacklist there is need of message set is used in system therefore easily user can block that person. System provides modified user wall by using filtering rules that means user has a control to change the setting according to his/her choice [8]. The system provides dominant filtering methods by which this content are not displayed on user's wall. In the system blocking of user for specific duration or lifetime before these warning is given to that particular person then blocks these people. There is three algorithms are used for filtering information[12]. Short text algorithm is initially used for filtration purpose when a message travels one user to another. Stemmer algorithm provides the estimation in this way process of linguistic forms, in which the alternating forms of a word are reduced to a common form. Stop word algorithm at this instant used for prevent the bad word in messages or comments which are posted on user walls[4].

III. SYSTEM OVERVIEW

System overview shows how the system works to avoid unwanted comments or messages. Private wall gives the control to the user for handling the unwanted messages automatically when he/she offline or online. Firewall means filtered wall contains the filtering rules which are used for filtering method when useless data gets posted on user's wall. Creator specification and online setup is done for user's threshold setting only for first appearance are two important filtering rules which is involved in this system.

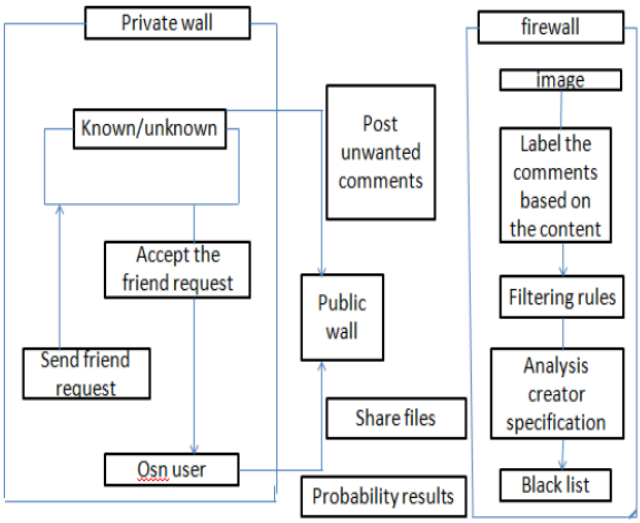

Figure 2: System Overview Diagram

Figure 2 shows how a system works and also shows the two wall architectures. How a system provides a flow of messages from source to destination i.e. one user to his/her known/unknown person. Private wall is used for show only malicious data on user's personal private wall which is confidential. Firewall means filtered wall which is used for showing only filtered messages on user wall. Filtering rules are main factor in the filtered wall for message filtration. Filtered wall is like boundary for user wall security.

 ISSN: 2321-8169
4086 - 4090

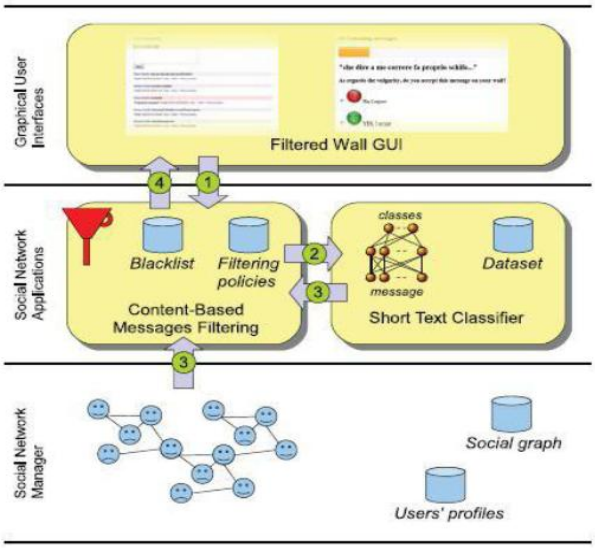

Figure 3: System Architecture Diagram

Figure 3 represents the system architecture of our proposed system. These are three layers are introduced in the proposed system:

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

SNM Provides essential OSN functionality and maintain a data regarding to user wall also provide basic OSN functionalities to support external applications.

Middle layer SNA is used for supporting middleware applications in OSN.

GUI used for setting up a filtering laws for filtered wall that is only show those messages which is user want to see.

IV. ALGORITHMIC STRATEGY

These are the 3 algorithms used in proposed system:

1. Short Text Algorithm
2. Stemmer Algorithm
3. Stop Word Algorithm

1. Short Text Algorithm:

Step 1: For any word of the short text, inquire the word pairs sets.
if there exists a record of a similar concept relationship,
go to step 5
else
if there exists a record of different concept relationships,
go to step 2
else
go to step 9;

Step 2: If there is only one word-pair Ti-tj,
go to step 4,
else
if there are several word-pairs,
go to step 3;

Step 3: Extract the right words of all the word-pairs related to ti and form into Tx,
if tj ∈ TX,
and
tj can be found in the vector space of this short text,
go to step 7,
else
extract tj , the right word of the word pair with the highest strength
and
go to step 4;

Step 4: Extract tj , the right word of this word-pair,
if
tj cannot be found in the vector space of this short text,
go to step 6,
else
go to step 7;

Step 5: Extract the word set TY in the text,
if
there exist tk ∈ TY and tk ∈ TZ
（attribute set of the word pair（ti,tj））,
go to step 8;
else
go to step 10;

Step 6: Calculate the mutual information between tj
and
other words in the text,
and
go to step 8
when meeting the requirements,
else
go to step 10;

Step 7: Calculate the mutual information between tj
and
other words in the text,
and
go to step 9
when meeting the requirements,
else
go to step 10;

 ISSN: 2321-8169
4086 - 4090

Step 8: Insert tj into the vector space of this short text;

Step 9: Raise the frequency of tj in the vector space of this Text at λ. (0<λ<1);

Step 10: Don't extend this word, and input and seek the next word.

2. Stemmer Algorithm

Step 1: Gets rid of plurals and -ed or -ing suffixes
Step 2: Turns terminal y to i when there is another Vowel in the stem
Step 3: Maps double suffixes to single ones: -ization, -ational, etc.
Step 4: Deals with suffixes, -full, -ness etc.
Step 5: Takes off -ant, -ence, etc.
Step 6: Removes a final -e

3. Stop words Algorithm

Step 1: T' ← Ø
Step 2: W= the set of all words in the domain
Step 3: D=T ∩ W
Step 4: Pick word w ∈ D
Step 5: For each interface q ∈ QI
Step 6: Remove w from the labels of interface q

Step 7: Check the stop word constraints for the labels of sibling nodes
Step 8: if no stop word constraint is violated then
T'←T' U {ω};
Else remove antonyms of w appearing in D from T'
Step 9: goto 4
Step 10: return T';

V. IMPLEMENTATION DETAILS

Implementation details contain basic modules included in system. Personalized message filtration system includes two modules:

A. System based application

System based application is simple application in which two types of filtering approaches includes are as follows-

1. General user wall (Unfiltered Wall)

General wall provides ability to user to show all the contents on his/her OSN wall. In that also mentioned about all the domains like vulgar, malicious content.

2. User's Secure Wall (Filtered Wall)

In this section system provides a control to user for selection of a particular domain. Also provides reliability to user for showing only those friends which is seen by user's view on private OSN wall. Filtered messages show in this section.

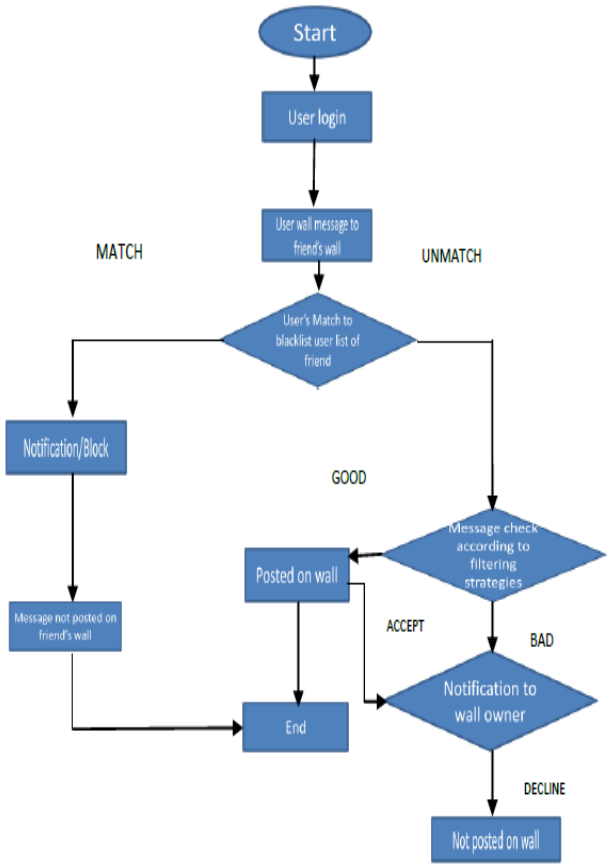

Figure 3. Filtering Approaches

Figure 3. Shows how to decide a message good or bad for filtration. If the known/unknown person is already in blacklist then gives the notification to that person or block that person due to this setting messages of that person is not posted on user's wall. Messages are check according to filtering strategies whether message is good or bad then and then it will be posted on user's wall of OSN.

B. Mobile based application

Mobile app module is based on android technology. Hence user can use this system on mobile outside whenever on his/her choice. Also used for users current position at that moment. In this implementation section system provides reliability to user in case of Mobile based application is supported all the versions of android.

VI. CONCLUSION

Hence system provides security for multiple peoples who use social networking for different purpose. As system can automatically filters unwanted messages from OSN by using short text algorithm and compare words by using stemmer algorithm for finding malicious data. Then compare words are eliminated or block by using stop word algorithm. System also helps in deciding whenever user should be inserted into a black list. User can identify a trust factor among all the friends. System focus on network message delivered based on OSN walls automatic removal of

 ISSN: 2321-8169
4086 - 4090

unnecessary messages from buffer overflow in filtered walls.

REFERENCES

[1] A. Adomavicius, G.and Tuzhilin, "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, vol. 17, no. 6, pp. 734–749, 2005.

[2] M. Chau and H. Chen, "A machine learning approach to web page filtering using content and structure analysis," Decision Support Systems, vol. 44, no. 2, pp. 482–494, 2008.

[3] 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, pp.195–204.

[4] F. Sebastiani, "Machine learning in automated text categorization,"ACM Computing Surveys, vol. 34, no. 1, pp. 1–47, 2002.

[5] 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.

[6] N. J. Belkin and W. B. Croft, "Information filtering and information retrieval: Two sides of the same coin?" Communications of the ACM, vol. 35, no. 12, pp. 29–38, 1992.

[7] P. J. Denning, "Electronic junk," Communications of the ACM, vol. 25, no. 3, pp. 163–165, 1982.

[8] P. W. Foltz and S. T. Dumais, "Personalized information delivery: An analysis of information filtering methods," Communications of the ACM, vol. 35, no. 12, pp. 51–60, 1992.

[9] P. S. Jacobs and L. F. Rau, "Scisor: Extracting information from online news," Communications of the ACM, vol. 33, no. 11, pp. 88–97, 1990.

[10] S. Pollock, "A rule-based message filtering system," ACM Transactions on Office Information Systems, vol. 6, no. 3, pp. 232–254, 1988.

[11] P. E. Baclace, "Competitive agents for information filtering," Communications of the ACM, vol. 35, no. 12, p. 50, 1992.

Gaurav N. Gharte he is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. His interest in the field of security.

Bhuvaneshwari B. Ugale she is student of Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest in the field of security.

Bhagyashri B. Pagar she is student of Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of pune. Her interest in the field of security.

K. S. Kumavat, ME, BE Computer Engg. Was educated at Pune University. Presently she is working as Head Information Technology Department of Brahma Valley College of Engineering and Research Institute, Nasik, Maharashtra, India. She has presented papers at National and International conferences and also published papers in National and International Journals on various aspects of Computer Engineering and Networks. Her areas of interest include Computer Networks Security and Advance Database.