Flexibility enhanced security system for OSN user wall

S.Subitha[*1], R.Umamaheswari[*2], M.L.Alphin Ezhil Manuel[#3]

[*1,*2]*U.G Student, B.E CSE, Alpha College of Engg, Chennai, T.N, India.*
[#3]*Assistant Professor, Dept of CSE, Alpha College of Engg, Chennai, T.N, India.*

[1]*radhauma21@gmail.com*

Abstract – Online Social Networks(OSN) is a feature in many social network services which allow users to create ,post ,comment to and read from their own interest. Before user have to take decision to accept or reject message through some filtering rules. Wall owner to specify BL rules regulating who has to be banned from their walls and for how long. Based on database word probability assign threshold for particular user to be blocked or send just notification message. White List is a list of those that are being provided a privilege and access to send a message .But BL easily fake any sender address and WL big risk of losing legitimate. In this paper we propose Bypassing filtering system to resolve the disadvantages of both BL and WL.

Keywords – OSN,FW,BL,WL, Bypass filtering system.

I. INTRODUCTION

ONLINE Social Networks (OSNs) are today one of the most popular interactive medium to communicate, share, and disseminate a considerable amount of human life information. Daily and continuous communications imply the exchange of several types of content, including free text, image, audio, and video data. According to Facebook statistics1 average user creates 90 pieces of content each month, whereas more than 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) are shared each month. The huge and dynamic character of these data creates the premise for the employment of web content mining strategies aimed to automatically discover useful information dormant within the data. They are instrumental to provide an active support in complex and sophisticated tasks involved in OSN management, such as for instance access control or information filtering. Information filtering has been greatly explored for what concerns textual documents and, more recently, web content (e.g., [1], [2], [3]). However, the aim of the majority of these proposals is mainly to provide users a classification mechanism to avoid they are overwhelmed by useless data. In OSNs, information filtering can also be used for a different, more sensitive, purpose. This is due to the fact that in OSNs there is the possibility of posting or commenting other posts on particular public/private areas, called in general walls. 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 believe that this is a key OSN service that has not been provided so far. Indeed, today OSNs provide very little support to prevent unwanted messages on user walls. 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 content-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. Providing this service is not only a matter of using previously defined web content mining techniques for a different application, rather it requires to design ad hoc classification strategies. This is because wall messages are constituted by short text for which traditional classification methods have serious limitations since short texts do not provide sufficient word occurrences. The experiments we have carried out show the effectiveness of the developed filtering techniques. In particular, the overall strategy was experimentally evaluated numerically assessing the performances of the ML short classification stage and subsequently proving the effectiveness of the system in applying FRs. Finally, we have provided a prototype implementation of our system having Facebook as target OSN, even if our system can be easily applied to other OSNs as well. To the best of our knowledge, this is the first proposal of a system to automatically filter unwanted messages from OSN user walls on the basis of both message content and the message creator relationships and characteristics.

The current paper substantially extends [4] for what concerns both the rule layer and the classification module. Major differences include, a different semantics for filtering rules to better fit the considered domain, an online setup assistant (OSA) to help users in FR specification, the extension of the set of features considered in the classification process, a more deep performance evaluation study and an update of the prototype implementation to reflect the changes made to the classification techniques. The remainder of this paper is organized as follows: surveys related work, whereas introduces the conceptual architecture of the proposed system. ML-based text classification method used to categorize text contents, whereas illustrates FRs and BLs. illustrates the performance evaluation of the proposed system, whereas the prototype application .

II. RELATED WORKS

The problem of [1] is collaborative methods, sufficient user data is available but not effective content information. The solution is ,using content based methods sufficient user data is unavailable but effective content information is easy to obtain. The problem of [2] is how to filter out irrelevant document from a set of document collected from the web. The solution is, Machine Learning based approach, that combine web content analysis, and web structure analysis. The problem of [3] is Human-engineered rule based systems, requiring many man-years to read document successfully. The solution is, Automatic classification patens that can be used for general document categorization or personalized filtering. The problem of [4] is existing policy-configuration tools are difficult for average users to understand and use. The solution is automatically configure the user detailed privacy settings using active learning algorithm.

III. DESIGN AND IMPLEMENTATION

A. Filtering Rules (FR):

FR's should allow user to state constraints on message creators. Possible to define rules by applying only to creators with a unwanted messages such as violence, vulgar, offensive(idiot),hate. A filtering rule FR is a tuple (author, creatorSpec, contentSpec, action), where

- author is the user who specifies the rule;
- creator Spec is a creator specification content Spec is a Boolean expression defined on content constraints of the form(c,ml), where C is a class of the first or second level and ml is the minimum membership level threshold required for class C to make the constraint satisfied;
- action is belongs to fblock; notify denotes the action to be performed by the system on the messages matching content Spec and created by users identified by creator Spec.

B. Online Setup Assistant for FR's thresholds:

We address problem of setting threshold to FR's, by implementing with Filtered Wall on OSA procedure. OSA user with a set of message selected from dataset. user tells system take decision to accept or reject message.
The fuzzy set is computed as;

$$Fc=\sum_{Mc} Ø(ma,mb),\text{where}$$

$$Ø(ma,mb)=½ +\{-_{mb/10 \text{ if } ma=pass}^{mb/10 \text{ if } ma=filter}$$

C. BlackListS(BL):

BL mechanism to avoid messages from undesired creators.Wall owners to specify BL rules regulating who has to be banned from their wall and for how long(threshold).
A BL rule is a tuple (author, creatorSpec, creatorBehavior, T), where

- author is the OSN user who specifies the rule, i.e., the wall owner;
- creatorSpec is a creator specification creatorBehavior consists of two components

RFBlocked and minBanned. RFBlocked ¼ (RF, mode, window) is defined such that - RF ¼ #bMessages/#tMessages , where #tMessages is the total number of messages that each OSN user identified by creatorSpec has tried to publish in the author wall (mode ¼ myWall) or in all the OSN walls (mode ¼ SN); whereas #bMessages is the number of messages among those in #tMessages that have been blocked; window is the time interval of creation of those messages that have to be considered for RF computation; minBanned ¼ (min, mode, window), where min is the minimum number of times in the time interval specified in window that OSN users identified by creatorSpec have to be inserted into the BL due to BL rules specified by author wall (mode ¼ myWall) or all OSN users (mode ¼ SN) in order to satisfy the constraint.

- T denotes the time period the users identified by creatorSpec and creator Behavior have to be banned.

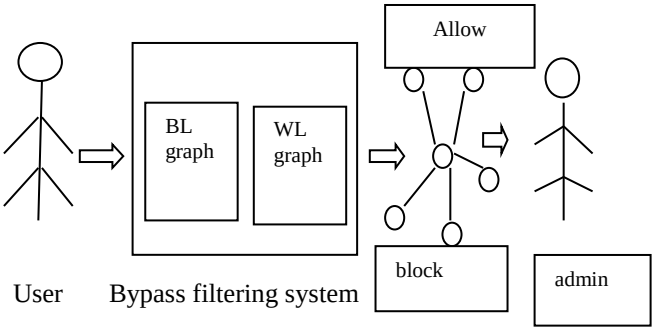
D. White Lists (WL):

WL that user are acceptable to send email. Disadvantage in WL big risk of losing legitimate user. List with profile, identity, reputation, trust, wherein said e-mail classification result and said e-mail classification result represent probabilities P_1 and P_2, respectively, and said single, aggregated e-mail classification value represents a combined probability Combined, and wherein said fuzzy logic-based voting mechanism includes a voting formula comprising:

P combined$=(P_1 \times P_2)/((P_1 \times P_2)+(1-P_1)(1-P_2))$.

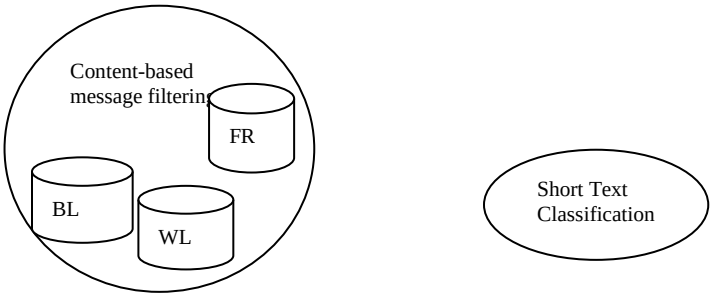
E. Bypass FilteringSystem:

Bypass filtering technique-BL & WL both viewed together as graph (social network manager). Bypassing the filtering system we get flexible enhanced secured system for OSN user wall.



The fastest possible algorithm for calculating the Levenshtein distance between
s1 ands2
|s1|>|s2| runs in:

O([s1])*max(1,|s2|/log[s1]))



Graphical user

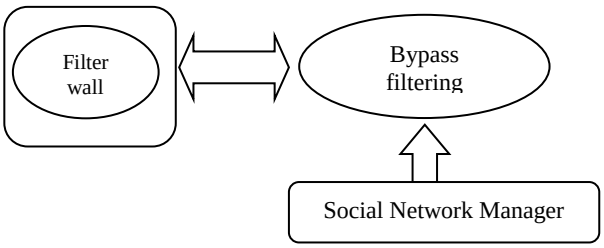


Fig .1. System Architecture

V. CONCLUSION & FUTURE WORK

User has been inserted into a BL for several times. System automatically send notification messages. Greater than a given threshold. User behavior is not improved and the system will be block the profile of particular user. Examine IP allow list easily fake any sender address. (BL wrongly estimates spammers). Whitelist with profile, identity, reputation, trust list.(WL risk of losing legitimate user).Using bypass filtering techniques, social network manager block correct user and also without losing legitimate user. The future works is to increase the accuracy of blacklists virtually eliminating false positives.

REFERENCES

[1] R.J. Mooney and L. Roy, "Content-Based Book Recommending Using Learning for Text Categorization," Proc. Fifth ACM Conf. Digital Libraries , pp. 195-204, 2000.

[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]. C.Apte, F.Damerau, S.M.Weiss, D.Sholom, M.Weiss," Automated Learning of Decision Rules for Text Categorization,"Trans.Information Systems,vol. 12,no.3,pp. 233-251,1994.

[4]. L. Fang and K. LeFevre, "Privacy Wizards for Social NetworkingSites," Proc. 19th Int'l Conf. World Wide Web (WWW '10), pp. 351-360, 2010

[5] F. Sebastiani, "Machine Learning in Automated Text Categorization," ACM Computing Surveys, vol. 34, no. 1, pp. 1-47, 2002.

[6] M. Vanetti, E. Binaghi, B. Carminati, M. Carullo, and E. Ferrari,"Content-Based Filtering in On-Line Social Networks," Proc.ECML/PKDD Workshop Privacy and Security Issues in Data Mining and Machine Learning (PSDML '10), 2010.

[7] P.W. Foltz and S.T. Dumais, "Personalized Information Delivery:An Analysis of Information Filtering Methods," Comm. ACM,vol. 35, no. 12, pp. 51-60, 1992.

[8] V. Bobicev and M. Sokolova, "An Effective and Robust Method for Short Text Classification," Proc. 23rd Nat'l Conf. Artificial Intelligence (AAAI), D. Fox and C.P. Gomes, eds., pp. 1444-1445, 2008.

[9] F. Bonchi and E. Ferrari, Privacy-Aware Knowledge Discovery: Novel Applications and New Techniques. Chapman and Hall/CRC Press,2010.

[10] J.A. Golbeck, "Computing and Applying Trust in Web-Based Social Networks," PhD dissertation, Graduate School of the Univ.of Maryland, College Park, 2005.