International Journal of Science Engineering and Advance Technology

A Novel Method for Providing Discrete Filtering and Blacklisting Options for OSN Users

Gadde.Sai Sudha, K.Priyanka
Student , Assistant Professor ,
Andhra Loyola Institute Of Engineering And Technology, Vijayawada.

ABSTRACT

OSN has fabulous growth in recent years interacting millions of users. OSNs are provided with viewing friends content and sharing so much of information and messages among the users and users are allowed write something on other users walls. So here the users may lose privacy by writing something bad and unwanted content on their walls.

Introducing access control which includes flexible rule based system as well as machine learn based soft classifier for posted messages control on user own walls. To overcome this problem, in this paper we are introducing a concept of Individual Filtering option to each and every user of the OSN to control the content being posted on their wall. Also an option which can restrict the other users from commenting on the user's wall, known as Blacklisting.

Keywords: Filtering Rule, Black List, Social Network Application, Content Based Message Filtering.

I.INTRODUCTION

Today's modern life is totally based on Internet. Now-a-days people cannot imagine life without Internet. Also, OSNs are just a part of modern life. From last few years most of the people are sharing their views, ideas, information (text, image, audio and video data) with each other using social networking sites. But, in today's OSN, there is a very high chance of posting unwanted content on particular public/private areas, called in general walls. So, to control this type of activity and prevent the unwanted messages which are written on user's wall we can implement Filtering Rules (FR) in our system. Also, Black List (BL) will maintain in this system. It can be used to give users the ability to automatically control the messages written on their own walls, by filtering out unwanted messages. 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.

OSNs provide support to prevent unwanted messages on user walls. 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 adhoc 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.

This is due to the fact that in OSNs there is possibility or commenting on other posts particularly public/private areas, called in general walls . For example, Face book allows user to state who is allowed to insert message in their walls (i.e., friends, friends of friends, or defined groups of friends). However no content based preference is 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 [3].

Besides classification facilities, the system provides a powerful rule layer exploiting a flexible language to specify Filtering Rules (FRs), by which users can state what contents, should not be displayed on their walls. FR can contain different criteria to customize according to user needs more precisely, FRs exploits user relationships user profiles as well as user defined Blacklists (BLs).

The remainder of this paper is organized as follows:
Section 2 Overview of the system, whereas Section 3 introduces the concept of the proposed system and section 4 reviews the implementation process. Finally, Section 5 concludes the paper.

II. SYSTEM OVERVIEW

In previous work, M.Vanetti [3] proposed a system allowing OSN users to have a direct control on the messages posted on their walls. This is achieved through a flexible rule-based system, which allows users to customize the filtering criteria to be applied to their walls, and a Machine Learning-based soft classifier automatically labelling messages in support of content-based filtering. The

system exploits a ML soft classifier to enforce customizable content-dependent FRs. Moreover, the flexibility of the system in terms of filtering options is enhanced through the management of BLs.

The first concerns the extraction and/ or selection of contextual features that have been shown to have a high discriminative power. The second task involves the learning phase. Since the underlying domain is dynamically changing, the collection of pre classified data may not be representative in the longer term. The present batch learning strategy, based on the preliminary collection of the entire set of labelled data from experts, allowed an accurate experimental evaluation but needs to be evolved to include new operational requirements.

Before illustrating the architecture of the proposed system, we briefly introduce the basic model underlying OSNs. In general, the standard way to model a social network is as directed graph, where each node corresponds to a network user and edges denote relationships between two different users. In particular each edge is labelled by the type of the established relationship (e.g., friend of, colleague of, parent of) and, possibly, the corresponding trust level, which represents how much a given user, considers trust worthy with respect to that specific kind of relationship the user with whom he/she is establishing it.

Therefore, there exists a direct relationship of a given type RT and trust value X between two users, if there is an edge connecting them having the labels RT and X. Moreover, two users are in an indirect relationship of a given type RT if there is a path of more than one edge connecting them, such that all the edges in the path have label RT. In general, the architecture in support of OSN services is a three-tier structure. The first layer commonly aims to provide the basic OSN functionalities (i.e., profile and relationship management).

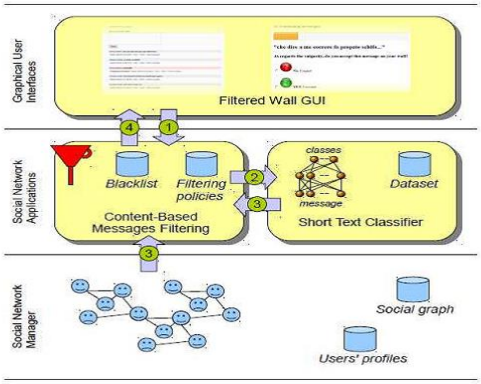

Figure 1.Filtered Wall Architecture

Additionally, some OSNs provide an additional layer allowing the support of external Social Network Applications (SNA) .Finally the supported SNAs may require an additional layer for their needed graphical user interfaces (GUIs). According to this reference layered architecture, the proposed system has to be placed in the second and third layers (Figure 1), as it can be considered as SNA. In particular, users interact with the system by means of a GUI setting up their filtering rules, according to which messages have to be filtered out. Moreover, the GUI provides users with a FW, which is a wall where only messages that are authorized according to their filtering rules are published [3].

The core components of the proposed system are the Content-Based Messages Filtering (CBMF) and the Short Text Classifier (STC) modules . The latter component aims to classify messages according to a set of categories [3].

By exploiting BLs, the system can prevent messages from undesired users. More precisely, the system is able to detect who are the users to be inserted in the BL according to the specified user preferences, so to block all their messages and for how long they should be kept in the BL.

III. PROPOSED SYSTEM

In this section, we describe the rule layer adopted for filtering unwanted messages. We start by describing FRs, and then we illustrate the use of BLs.

In this paper, we are introducing a new approach towards this problem, where there is an individual decision making facility for users of OSN in filtering words. Even there is also choice for the OSN users to select the applicability of the word to ALL friends or to a Specific friend. Also regarding Blacklists, user can choose the Blacklisting users from user's friends list and will also have an option of unblocking them if required.

We model a social network as a directed graph, where each node corresponds to a network user and edges denote relationship between two different users. Without loss of generality, we suppose that trust levels are rational number in the range [0, 1]. Moreover two users are in an indirect relationship of a given type RT if there is a path of more than one edge connecting them, such that all the edges in the path have label RT.

A. Filtering Rules

In defining the language for FRs specification, we consider three main issues that, in our opinion, should affect a message filtering decision.

i. If the mentioned user is already blacklisted, then there is no need to enter into the filtering policies.
ii. When a user tries to comment on the wall of his friend, the message has to be filtered according to the receiver's filter.
iii. Each user can have their own restricted text to be filtered, which is applicable only to those who try to post a comment on their wall and friend of them.

In detail about the content stored as Filter, related to user is a tuple of (CreatorSpec, Word, Type, Applicability)

a. CreatorSpec is the specification of the user who creates this filter.
b. Word indicates the word which should be filtered in the message and by default if the word is found it gives a warning message to the user trying to post it.
c. Type is the category under which the word comes under.
d. Applicability means the filter to be applied to a single user or ALL the friends of the user.

B. Blacklists

We make use of a BL mechanism to avoid messages from undesired creators. Each user is provided with their own blacklists and can have an option of making changes in future if required.

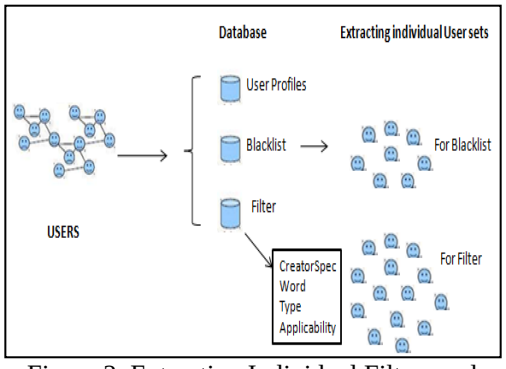

Figure 2. Extracting Individual Filters and Blacklists for the Users.

In Figure2, the individual datasets extraction is shown from a common huge dataset. Each user can apply any modifications on their data, which is created by them. These user data sets are used while any transaction is happening concerned with the user.

Advantages:

1. Users can have their own choice regarding the applicability of the filter.
2. User can have his/her own filter which is opted by his/her interest.
3. Blacklisted users can be restricted from commenting on user's wall who blacklisted them.
4. Each time user can update his/her filter and blacklist by their choice.

IV. IMPLEMENTATION PROCESS

In this section, the actual procedure which takes place is explained. The main concern with this proposed system is the process of the filtering and blacklisting. The message sent by the sender undergoes some verification and then it may be posted on the wall of the receiver or discarded according to the result of verification..

All Users of the system can use the options provided by the system to them. In a sequence the steps, user may go through are

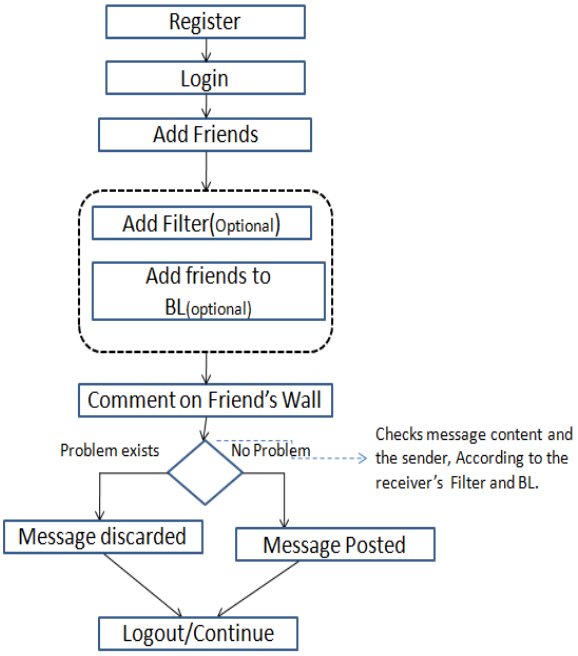

Figure 3. Flow of Activities.

In Figyre 3, the following steps are shown.

i) User gets registered to the system.

ii) User logs into the system.

iii) User adds the other users available in the network as friends according to user's wish.

iv) User may make use of the options available for filtering and also blacklisting option.

v) When he/she tries to comment on other's wall then, the sender will be the current user, and the receiver is the destination user to whom this message has to be posted.

vi) In this checking the sender is checked with the list of users blacklisted in the receiver's blacklist. If match is found then message is discarded and cannot be posted, as the sender is blacklisted by the receiver.

vii) If the sender is not blacklisted by the receiver, then the other check has to be made, this time it is for the message/ content of the comment to be posted to the receiver. This check is made with the filter of the receiver, if the message contains any of the words blocked by the receiver. If match is found then the message will be discarded due to the content not acceptable by the receiver.

viii) Finally after the verification and testing is done, the message is either posted on the receiver's wall or discarded at the sender's end itself. Next the User may choose to continue some transactions or logout of the session.

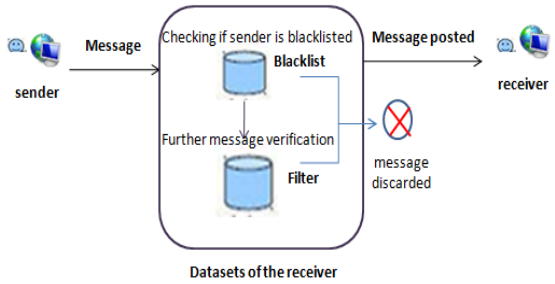

Figure 4. Message Verification Process

In the Above Figure4, the message/comment content is verified by using two different datasets of the receiver.

One is with the Blacklist dataset, and the other is with the Filter dataset of the receiver.

Depending up on the result of the verification process, the message is decided to be posted or discarded.

This is about how the filtering and blacklisting mechanisms are performed on data and these also play an important role in the life of OSNs. Helping users in identifying what are their requirements and preferences regarding the data posting on their wall and can also be choosy about persons posting comments on their wall

V. CONCLUSION

In this paper we have shown a solution for the problem of message filtering and blacklisting users. There may be other ways to solve the same problem in a different way, for a better solution.

Future enhancements for this system might be solving a similar problem to this like image filtering containing message and also in other way restricting the posting of one user's image by the other without proper permission from the owning user. Even more, filtering techniques may improve in the near future so that more user-friendly options can be added to the proposed system.

Finally we conclude that our proposed system is used to filter undesired messages from OSNs wall using customizable Filtering Rules (FR) enhancing through Blacklists (BLs).

REFERENCES

[1] 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.

[2] N.J. Belkin and W.B. Croft, "Information Filtering and Information Retrieval: Two Sides of the Same Coin?" Comm. ACM, vol. 35, no. 12, pp. 29-38, 1992.

[3] Marco Vanetti, Elisabetta Binaghi, Elena Ferrari, Barbara Carminati, and Moreno Carullo," A System to Filter Unwanted Messages from OSN User Walls" IEEE, VOL. 25, NO. 2, FEBRUARY 2013.

[4] 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.

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

[8] 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.

[9] Hanani, U., Shapira, B., Shoval, P.: Information filtering: Overview of issues, research and systems. User Modeling and User-Adapted Interaction 11, 203–259 (2001).

[10] B. Sriram, D. Fuhry, E. Demir, H. Ferhatosmanoglu, and M.Demirbas, "Short Text Classification in Twitter to Improve Information Filtering," Proc. 33rd Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR '10), pp. 841-842, 2010.

[11] Manning, C., Raghavan, P., Schutze, H.: Introduction to Information Retrieval. Cambridge University Press, Cambridge, UK (2008).

Gadde.Sai Sudha, is a student of Andhra Loyola Institute Of Engineering And Technology (ALIET), Vijayawada. Under JNTUKakinada. She received her B.Tech in IT from ALIET, Vijayawada .Presently she is pursuing her M.Tech (CSE) from this college. Interested areas are Data Mining, DBMS and Object oriented Programming languages, some current trends and techniques in Computer Science.

K.Priyanka received M.Tech.(CSE) from KLUniversity, Vaddeswaram. Presently working as Asst. Prof., Dept of CSE,ALIET, Vijayawada, A.P. Interested in Data Mining and Data Warehousing. She has published papers in 4 National Journals.