RESEARCH ARTICLE OPEN ACCESS

Filter False Message from User Wall

Sunanda Reddy, Gourav Jain, Deepesh Wairkar, Vinay Haram, Prof. Gayatri Naik
YadavraoTasgaonkar Institute of Engineering & Technology
Chandhai, Nasrapur
Karjat, Raigad - 410 201
Maharashtra – India

ABSTRACT
Online Social Networks (OSNs) are today one of the most popular interactive medium. We can use OSNs to communicate with people and to share information from one person to another. Most of the messages are avoided due to social issues and for that filtering is the most important aspect. This can lead to a fact that anyone can post in public/private walls of user. Hence, Filtering of messages would be useful to manage the private/public user walls and filter the entire false message and make it safe to be readable. OSNs provide very little support to prevent unwanted messages on user walls. For instance, Facebook permits users to state who is allowed to insert messages in their walls (i.e., friends, defined groups of friends or friends of friends). Though, no content-based partialities are preserved and therefore it is not possible to prevent undesired communications, for instance political or offensive ones, no matter of the user who posts them. So to avoid this, filtering system is used which will filter this false message and avoid it to be posted on user wall.
Keywords:- SNM, SNA, GUI

I. INTRODUCTION

In the last years, On-line Social Networks (OSNs) have become a popular interactive medium to communicate, share information. Daily and continuous communication implies the exchange of several types of content, including free text, image, audio and video data. The huge and dynamic character of these data automatically discover useful information within the data and then provide an active support in complex and manage the false message to be posted. A main part is constituted by short text, a notable example are the messages permanently written by OSN users on particular public/private areas, called in general walls.

The aim of the present work is to propose and experimentally evaluate an automated system, called Filtered Wall (FW), able to filter out false messages from social network user walls. The key idea of the proposed system is to avoid the false messages to be displayed by maintaining a database of the string and comparing it with the messages posted on the users private/public wall. This would avoid the false messages and the message displayed would be safe. 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. For instance, it is not possible to prevent political or vulgar messages. In contrast, by means of the proposed mechanism, a user can specify what contents should not be displayed on his/her wall, by specifying a set of filtering rules. Filter ing 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, as well as the output of the ML (Machine Language) categorization process. 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.

II. LITERATURE REVIEW

The main goal of information filtering system is to filter unwanted content from input data before its presentation to the end user. It takes into account user profile and Compares it with referred characteristics or properties. For filtering of messages there are different filtering methods as follows:

(A) Content-based filtering

Content-based filtering, also referred to as cognitive filtering, recommends items based on a comparison between the content of the items and a user profile. The content of each item is represented as a set of descriptors or terms, typically the words that occur in a document. The user profile is represented with the same terms and built up by analyzing the content of items which have been seen by the user.

Several issues have to be considered when implementing a content-based filtering system. First, terms can either be assigned automatically or manually. When terms are assigned automatically a method has to be chosen that can extract these terms from items. Second, the terms have to be represented such that both the user profile and the items can be compared in a meaningful way. Third, a learning algorithm has to be chosen that is able to learn the user profile based on seen items and can make recommendations based on this user profile.

(B) Collaborative filtering

Collaborative filtering has two senses, a narrow one and a more general one [2]. In general, collaborative filtering is the process of filtering for information or patterns using techniques involving collaboration among multiple agents, viewpoints, data sources, etc. [2]. Applications of collaborative filtering typically involve very large data sets. Collaborative filtering methods have been applied to many different kinds of data including: sensing and monitoring data, such as in mineral exploration, environmental sensing over large areas or multiple sensors. For example, a collaborative filtering recommendation system for television tastes could make predictions about which television show a user should like given a partial list of that user's tastes (likes or dislikes).

C. Policy-based personalization

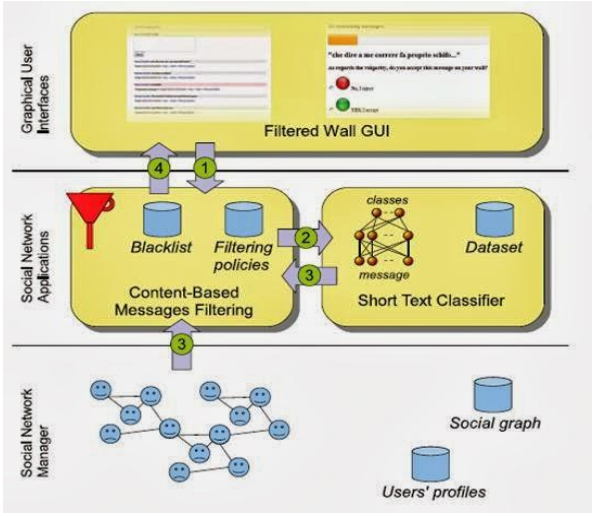
Policy based personalization is according user defined policies. In online social networking sites user oriented policies can define how communication between two parties or more can be handled. The policy based personalization system in focuses on Twitter2 [3].It assigns a category to each tweet and shows only those tweet to the user which are of his interest.

III. ARCHITECTURE OF FILTER WALL

1. Social Network Manager (SNM)

The initial layer is Social Network Manager layer 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 Rules (FR) and Black lists (BL).

2. Social Network Application (SNA)



In second layer Content Based Message Filtering (CMBF) and Short Text Classifier is composed. This is very important layer for the message categorization according to its CBMF filters. Also Black list is maintained for the user who sends frequently bad words in message.

3. Graphical User Interface (GUI)

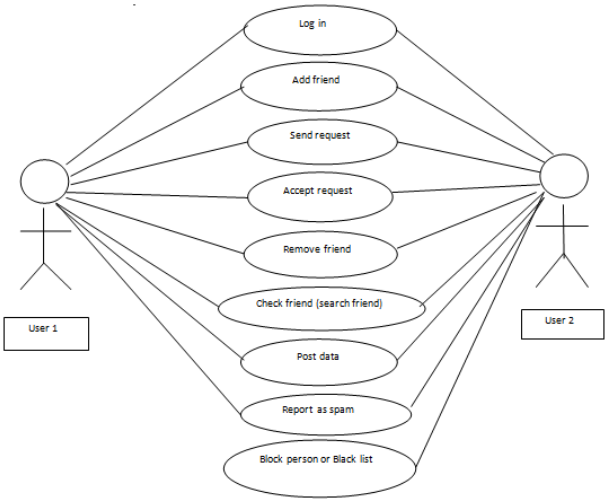
Third layer provides Graphical User Interface to the user who wants to post his messages as a input. In this layer Filtering Rules (FR) are used to filter the unwanted messages and provide Black list (BL) for the user who are temporally prevented to publish messages on user's wall.

4. Blacklist

A further component of our system is a BL mechanism to avoid messages from undesired creators, autonomous from their substances. BLs is straightly supervised by the system, which should be able to establish who are the users to be introduced in the BL and decide when users retention in the BL is completed. To improve flexibility, such information is providing to the system during a set of rules, after this called BL rules. Such rules are not defined by the SNMP; thus, they are not meant as common high-level directives to be practical to the entire society. Rather, we choose to permit the users themselves, i.e., the wall's owners to indicate BL rules regulating who has to be banned from their walls and for how lengthy. Consequently, a user might be eliminated from a wall, by, at the same time, being capable to post in other walls.

IV. DESIGN USE CASE DIAGRAM

The use case diagram for the online social networking user wall is as follows:



Use Case Diagram for user walls

V. CONCLUSION

Thus with this methodology we can provide unwanted or false messages to be displayed on public/private user wall. Filtering the messages stored in the database will help users to select which messages to be displayed on the users wall and which messages need not be displayed. With this the person can use the online social network without any problems to the end user and can communicate safely from one user to another. The user can also decide with which user to communicate with and also have the authority to black list the person if the person misuses the social network. This can make a safe communication and sharing of information without misuse.

VI. FUTURE SCOPE

1. This application would avoid all the false messages (sexual, vulgar, political, abusive, etc.).
2. This facility would provide protection to avoid his wall from any type of malpractices.
3. If the abusive words are used for the given n number of times that person is marked as spam and blacklisted by blocking them.

ACKNOWLEDGEMENT

We are immensely obliged to Prof. Gayatri Naik for his immense support for the project and for his guidance and supervision. It has indeed been a fulfilling experience for working out this project report. Lastly, we thank almighty & our parents, for their constant encouragement without which this project would not be possible.

REFRENCE

[1.] Marco Vanetti, Elisabetta Binaghi, Elena Ferrari, Barbara Carminati, and Moreno Carullo- IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 2, FEBRUARY 2013.

[2.] Amati, G., Crestani, F.: Probabilistic learning for selective dissemination of information. Information Processing and Management 35(5), 633–654 (1999)

[3.] Boykin, P.O., Roychowdhury, V.P.: Leveraging social networks to fight spam. IEEE Computer Magazine 38, 61–67 (2005)

[4.] Carminati, B., Ferrari, E.: Access control and privacy in web-based social networks. International Journal of Web Information Systems 4, 395–415 (2008)

[5.] Carminati, B., Ferrari, E., Perego, A.: Enforcing access control in web-based social networks. ACM Trans. Inf. Syst. Secur. 13(1), 1–38 (2009)

[6.] Carullo, M., Binaghi, E., Gallo, I.: An online document clustering technique for short web contents. In: Pattern Recognition Letters. vol. 30, pp. 870–876 (July 2009)

[7.] Churcharoenkrung, N., Kim, Y.S., Kang, B.H.: Dynamic web content filtering based on user's knowledge. International Conference on Information Technology: Coding and Computing 1, 184–188 (2005)

[8.] Fang, L., LeFevre, K.: Privacy wizards for social networking sites. In: WWW '10: Proceedings of the 19th international conference on World wide web. pp. 351–360. ACM, New York, NY, USA (2010)

[9.] Fong, P.W.L., Anwar, M.M., Zhao, Z.: A privacy preservation model for facebook-style social network systems. In: Proceedings of 14th European Symposium on Research in Computer Security (ESORICS). pp. 303–320 (2009)

[10]. Frakes, W., Baeza-Yates, R. (eds.): Information Retrieval: Data Structures & Algorithms. Prentice-Hall (1992)

[11] A. Adomavicius and G. Tuzhilin, "Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions," IEEE Trans. Knowledge and Data Eng., vol. 17, no. 6, pp. 734-749, June 2005.

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] P.J. Denning, "Electronic Junk," Comm. ACM, vol. 25, no. 3, pp. 163-165, 1982.

[18] 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.

[19] P.S. Jacobs and L.F. Rau, "Scisor: Extracting Information from OnLine News," Comm. ACM, vol. 33, no. 11, pp. 88-97, 1990.

[20] S. Pollock, "A Rule-Based Message Filtering System," ACM Trans. Office Information Systems, vol. 6, no. 3, pp. 232-254, 1988.

[21] P.E. Baclace, "Competitive Agents for Information Filtering,"