

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.767 – 772

RESEARCH ARTICLE

Filtered Wall: An Automated System to Filter Unwanted Messages from OSN User Walls

Ms. Pallavi Kalyane, Prof. Sachin Chavan, Prof. Pravin Rahate

Student, MGM CET, Department of Computer Engineering, University of Mumbai, India

Professor, MGM CET, Department of Computer Engineering, University of Mumbai, India

Professor, DMCE, Department of Computer Engineering, University of Mumbai, India

pallavi.kalyane@gmail.com; ssschavan2003@gmail.com; pravinsrahate@gmail.com

Abstract— Now days On-line Social Networks (OSNs) are one of the most popular interactive medium to communicate, share, and disseminate a considerable amount of human life information. This project represents a system enforcing filtering of unwanted messages coming from the user based on its content. Our system gives ability to OSN users to have a direct control on the messages posted on their walls. Up to now, OSNs provide little support to prevent unwanted messages on user walls. There is no content-based preferences are supported and therefore it is not possible to prevent unwanted 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. One fundamental issue in this system is blocking of user for lifetime. We overcome this Problem by using Proposed System; In this paper, we propose a system that performs blocking of user for particular time limit and also send notification, E-Mail to that who has posted unwanted message on wall. Along with that we are using Self Organizing Neural Network (SOINN) with Radial Based Function (RBF) for classification of text. In this we use the back propagation technique of neural network (i. e. Using previous knowledge of user messages we take proper action).

Keywords— Online social networks; Filtered Wall; Blacklists; Machine Learning text categorization

I. INTRODUCTION

On-line Social Networks (OSNs) are platforms that allow people to publish information about them and to connect to other users of the network through links. Now days, the popularity of OSNs is increasing significantly. Twitter, Facebook, LinkedIn have more than a hundred million active users. The existence of OSNs that include person- specific information creates both interesting opportunities and challenges. For example, data available on social network is useful for marketing products to the right customers. At the same time, security and privacy needs to be concerned. Improving the OSN access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. To address

some of these limitations, we propose an extensible, fine-grained OSN access control model based on semantic web technologies. Our main idea is to encode social network-related information by means of ontology [1]. Web-based Social Networks (WBSNs) are online communities that allow users to publish resources and to record and/or establish relationships with other users, such as friend, colleague, etc. for the purpose of business, entertainment, religion, etc. An increasing number of social networking and social media sites allow users to customize their own privacy policies. For example, Facebook has a Privacy Settings page, which allows users to specify which pieces of profile data each friend is allowed to view. Facebook also allows users to create friends list, and then specify whether a piece of profile data is visible or invisible to all friends in a particular list.

In the last years, On-line Social Networks (OSNs) have become a popular interactive medium to communicate, share and disseminate a considerable amount of human life information. Daily and continuous communication results in exchange of several types of content, including free text, image, and audio and video data. The huge and dynamic character of these data creates the need of web content mining strategies aimed to automatically discover useful information from the large amount of data and then provide an active support in complex and sophisticated tasks involved in social networking analysis and management. In OSNs, information filtering can be used for a different, 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 [11].

The aim of the present work is therefore to propose and experimentally evaluate an automated system, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. We exploit Machine Learning (ML) text categorization techniques to automatically assign with each short text message a set of categories based on its content [11]. Our focus in this work is on online identification of real-world event content. We identify each event and its associated Twitter messages using an online clustering technique that groups together topically similar tweets. We then compute revealing features for each cluster to help determine which clusters correspond to events. Importantly, we design features to distinguish between real-world events and a special family of non-events, namely, Twitter-centric or trending topics that carry little meaning outside the Twitter system. These Twitter-centric activities often share similar temporal distribution characteristics with real-world events, as discussed below. We also distinguish tweets between PESTEL (p-political, e-economical, s-social, t-technical, e-environmental, and l-legal).

II. LITERATURE SURVEY

In the literature survey we are going to discuss recent methods over the Content-based Filtering in On-line Social Networks. Below in literature we are discussing some of them.

- Carminati, B., Ferrari, [1] In this paper, they have proposed an extensible fine-grained online social network access control model based on semantic web tools. In addition, they propose authorization, administration and filtering policies that are modelled using OWL and SWRL. The architecture of a framework in support of this model has also been presented. Further, they have implemented a version of this framework and presented experimental results for the length of time access control can be evaluated using this scheme. Further work could be conducted in the area of determining a minimal set of access policies that could be used in evaluating access requests in a further attempt to increase the efficiency of these requests.
- [2] In this paper, they have proposed an access control model and related enforcement mechanism for WBSNs, which adopts a rule-based approach for specifying access control policies on the resources owned by network participants, and where authorized users are denoted in terms of the type, depth, and trust level of relationships. Differently from traditional access control systems, our mechanism makes use of a semi-decentralized architecture, where the information concerning users' relationships is encoded into certificates, stored by a certificate server, whereas access control enforcement is carried out client-side.
- Churcharoenkrung, N., Kim, Y.S., Kang, [3] This paper focuses on the development of a maintainable information filtering system. The simple and efficient solution to this problem is to block the Web sites by URL, including IP address. However, it is not efficient for unknown Web sites and it is difficult to obtain complete block list. Content based filtering is suggested to overcome this problem as an additional strategy of URL filtering. The manual rule based method is widely applied in current content filtering systems, but they overlook the knowledge acquisition bottleneck problems. To solve this problem, we employed the multiple classification ripple-down rules (MCRDR) knowledge acquisition method, which allows the domain expert to maintain the knowledge base without the help of knowledge engineers. Throughout this study, they prove the MCRDR based information filtering system can easily prevent unknown Web information from being delivered and easily maintain the knowledge base for the filtering system

- Fang, L., LeFevre, K. [4] Privacy is an important emerging problem in online social networks. While these sites are growing rapidly in popularity, existing policy configuration tools are difficult for average users to understand and use. This paper presented a template for the design of a privacy wizard, which removes much of the burden from individual users. At a high level, the wizard solicits a limited amount of input from the user. Using this input, and other information already visible to the user, the wizard infers a privacy-preference model describing the user's personal privacy preferences. This model, then, is used to automatically configure the user's detailed privacy settings.
- Fong, P.W.L., Anwar, M.M., Zhao, Z. [5] They have formalized the distinct access control paradigm behind the Facebook privacy preservation mechanism into an access control model, which delineates the design space of protection mechanisms under this paradigm of access control. They have also demonstrated how the model can be instantiated to express access control policies that possess rich and natural social significance.

III. PROBLEM DEFINITION

In these systems blocking of user is for lifetime. We overcome this Problem by using Proposed System. In our system we plan to block the user for particular time limit and also send notification, E-Mail sending to that who posted on wall. The application of content-based filtering on messages posted on OSN user walls poses further challenges given the short length of those messages apart from the wide range of topics that may be mentioned. Short text classification has received up to currently little attention within the scientific community. Recent work highlights difficulties in shaping robust options, basically as a result of the very fact that the description of the short text is crisp, with several misspellings, nonstandard terms, and noise. Our work is additionally galvanized by the various access management models and connected policy languages and social control mechanisms that are projected to date for OSNs since filtering shares many similarities with access management.

IV. PROPOSED SYSTEM

In this paper we are planning to block the user for particular time limit and also send notification, E-Mail sending to that user who posted on wall. Along with that we are using Self Organizing Neural Network (SOINN) with Radial Based Function (RBF) for classification of text. In this we use the back propagation technique of neural network (i. e. Using previous knowledge of user messages we take proper action).

A. ARCHITECTURE

The Filtered wall architecture in support of OSN services is a three-tier structure (see Fig. 1). The first layer, called Social Network Manager (SNM), it provides the basic OSN functionalities (i.e., profile and relationship management), whereas the second layer provides the support for external Social Network Applications (SNAs). The supported SNAs may in turn require an additional layer for their needed Graphical User Interfaces (GUIs). According to this reference architecture, the proposed system is placed in the second and third layers. In particular, users interact with the system by means of a GUI to set up and manage their FRs/ BLs. Moreover, the GUI provides users with a FW, that is, a wall where only messages that are authorized according to their FRs/BLs are published [11].

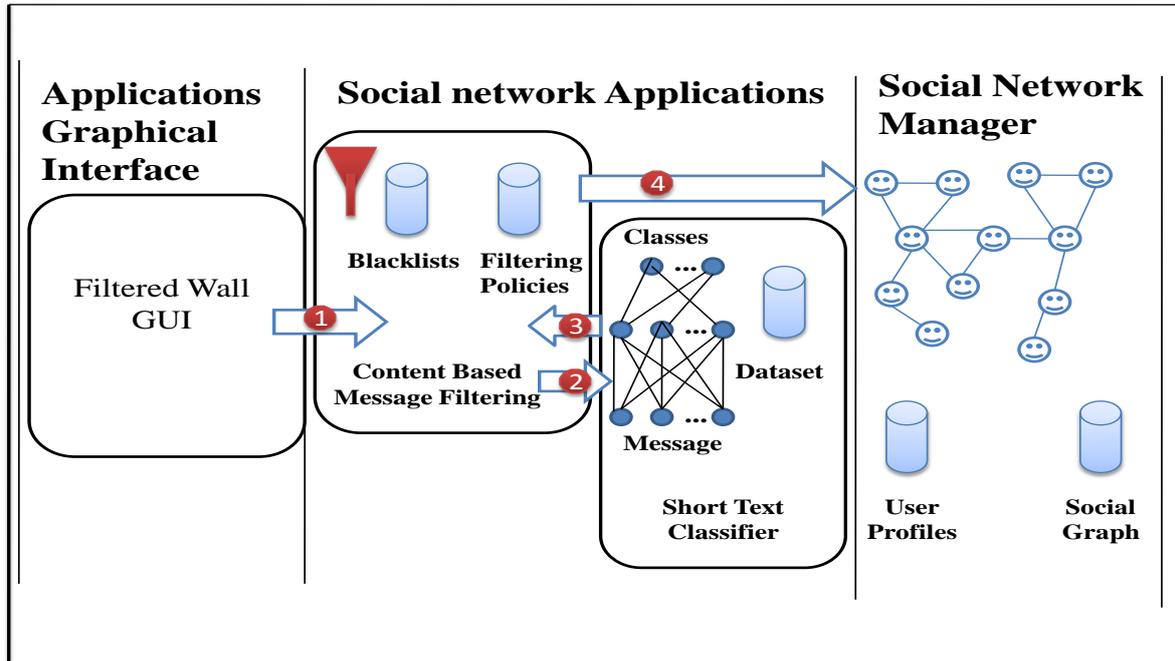


Fig.1 Architecture of Filtered Wall

The major efforts in constructing a robust and flexible short text classifier (STC) are concentrated in the extraction and selection of a set of characterizing and discriminant features. The solutions investigated in this paper are an extension of those adopted in a previous work by us from which we inherit the learning model and the elicitation procedure for generating preclassified data. The original set of features, derived from endogenous properties of short texts, is enlarged here including exogenous knowledge related to the context from which the messages originate. As far as the learning model is concerned, we confirm in the current paper the use of neural learning which is today recognized as one of the most efficient solutions in text classification. In particular, we base the overall short text classification strategy on Radial Basis Function Networks (RBFN) with Self Organizing Neural Network (SOINN) for their proven capabilities in acting as soft classifiers, in managing noisy data and intrinsically vague classes. Moreover, the speed in performing the learning phase creates the premise for an adequate use in OSN domains, as well as facilitates the experimental evaluation tasks. We insert the neural model within a hierarchical two level classification strategy. In the first level, the RBFN with Self Organizing Neural Network (SOINN) categorizes short messages as Neutral and Nonneutral; in the second stage, Nonneutral messages are classified producing gradual estimates of appropriateness to each of the considered category. 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. FRs can support a variety of different filtering criteria that can be combined and customized according to the user needs. More precisely, FRs exploit user profiles, user relationships as well as the output of the ML categorization process to state the filtering criteria to be enforced. If the friend of user continuously posts the unwanted messages of particular type on users wall then user will send the notification message to that user who posted on wall. In addition, the system provides the support for user-defined Blacklists (BLs), that is, list of users that are temporarily prevented to post any kind of messages on a user wall.

V. MACHINE LEARNING-BASED CLASSIFICATION

A hierarchical two level classification process is used for short text categorization. The first-level classifier performs a binary hard categorization that labels messages as Neutral and Nonneutral. After first-level filtering task there is subsequent second-level task in which a fine-grained classification is performed. The second-level classifier performs a soft classification of Nonneutral messages assigning a given message a gradual membership to each of the Nonneutral classes. Among the variety of multiclass ML models well suited for text classification, we choose the RBFN model [12] with Self Organizing Neural Network (SOINN) for the experimented competitive behaviour with respect to other state-of-the-art classifiers. RBFNs have a single hidden layer of processing units with local, restricted activation domain: a Gaussian function is commonly used, but any other locally tunable function can be used. They were introduced as a neural network evolution of exact

interpolation [13], and are demonstrated to have the universal approximation property [14], [15]. As outlined in [16], RBFN main advantages are that classification function is nonlinear, the model may produce confidence values and it may be robust to outliers; drawbacks are the potential sensitivity to input parameters, and potential overtraining sensitivity. The first-level classifier is then structured as a regular RBFN with Self Organizing Neural Network (SOINN). In the second level of the classification stage, we introduce a modification of the standard use of RBFN with Self Organizing Neural Network (SOINN). Its regular use in classification includes a hard decision on the output values: according to the winner-take-all rule, a given input pattern is assigned with the class corresponding to the winner output neuron which has the highest value. In our approach, we consider all values of the output neurons as a result of the classification task and we interpret them as gradual estimation of multimember ship to classes.

VI. FILTERING RULES

FRs allows users to state constraints on message creators. Creators on which a FR applies can be selected on the basis of several different criteria; one of the most relevant is by imposing conditions on their profile's attributes. In such a way it is, for instance, possible to define rules applying only to young creators or to creators with a given religious/political view. Creators may also be identified by exploiting information on their social graph. This implies to state conditions on type, depth, and trust values of the relationship(s) creators should be involved in order to apply them the specified rules [11]. All these options are formalized by the notion of creator specification, defined as follows:

Definition 1 (Creator specification): A creator specification creatorSpec denotes a set of OSN users. It can have one of the following forms, possibly combined:

1. A set of attribute constraints of the form $an \text{ OP } av$, where an is a user profile attribute name, av and OP are, respectively, a profile attribute value and a comparison operator, compatible with an 's domain.
2. A set of relationship constraints of the form $(m; rt; minDepth; maxTrust)$ denoting all the OSN users participating with user m in a relationship of type rt , having a depth greater than or equal to $minDepth$, and a trust value less than or equal to $maxTrust$.

Example 1: The creator specification $CS1 = \{Age < 16; Sex = male\}$ denotes all the males whose age is less than 16 years, whereas the creator specification $CS2 = \{Helen; colleague; 2; 0.4\}$ denotes all the users who are colleagues of Helen and whose trust level is less than or equal to 0.4. Finally, the creator specification $CS3 = \{(Helen; colleague; 2; 0.4); (Sex = male)\}$ selects only the male users from those identified by $CS2$ [11].

Definition 2 (Filtering rule): A filtering rule FR is a tuple $(author, creatorSpec, contentSpec, action)$, where

- $author$ is the user who specifies the rule;
- $creatorSpec$ is a creator specification, specified according to Definition 1;
- $contentSpec$ 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;
- $action: \{block; notify\}$ denotes the action to be performed by the system on the messages matching $contentSpec$ and created by users identified by $creatorSpec$.

VII. HARDWARE & SOFTWARE DESCRIPTION

A. Hardware Requirements:

Processor	:	Pentium IV 2.6 Ghz
Ram	:	512 Mb
Hard Disk	:	20 Gb
Floppy Drive	:	1.44 Mb
Keyboard	:	Standard 102 Keys
Mouse	:	3 Buttons

B. Software Requirements:

Front End	:	Java
Tools Used	:	Eclipse/Netbeans
Operating System	:	Windows 7

C. Application:

Following are some OSNs where Filtered wall is required to filter unwanted messages: Facebook, Twitter, Orcut, LinkedIn.

VIII. CONCLUSION

In this paper, we have presented Filtered Wall. The system exploits a ML soft classifier to enforce customizable content-dependent filtering rules. The flexibility of the system in terms of filtering options is enhanced through the management of BLs. System proposed in this paper represents just the core set of functionalities needed to provide a sophisticated tool for OSN message filtering with temporary blocking of user and also send notification, E-Mail to that who has posted unwanted message on wall. This might enhance services provided by OSN. BL and FR specification are made easier by development of GUI and a set of related tools. Along with it, our proposed system provides a better accuracy for classification of message as compare to previous implemented methods. The miss-classification of message is reduced by using RBF with NN. By computing matrix (FP, FN, TP, TN, precision and recall) we compare results with other classification techniques.

ACKNOWLEDGEMENT

I would like to take this opportunity to thank MGM trust and Principal DR. S.K Naranyankhedkar, MGM CET for giving me an opportunity to carry out my project work.

I express my deep sense of gratitude towards Prof. V. Balachandran, Head of the Department of Computer for his valuable guidance and encouragement. I wish to acknowledge my extreme gratitude to my guide Prof. Pravin Rahate, co-guide Prof. Sachin Chavan for guiding me throughout the work on project. I have been greatly benefited by his valuable suggestion and ideas.

REFERENCES

- [1] Carminati, B., Ferrari, E., "Access control and privacy in web-based social networks," International Journal of Web Information Systems, pp. 395–415, 2008.
- [2] Carminati, B., Ferrari, E., Perego, "Enforcing access control in web-based social networks," ACM Trans. Information System Security, pp. 1–38, 2009.
- [3] 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, pp. 184–188 2005.
- [4] 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.
- [5] 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.
- [6] Ali B., Villegas W., Maheswaran M., "A trust based approach for protecting user data in social networks;" In: Proceedings of the 2007 conference of the center for advanced studies, on Collaborative research, pp. 288–293. ACM, New York, NY, USA, 2007.
- [7] Amati, G., Crestani, F.: Probabilistic learning for selective dissemination of information. Information Processing and Management 35(5), 633–654 (1999)
- [8] Boykin, P.O., Roychowdhury, V.P. "Leveraging social networks to fight spam. IEEE Computer Magazine 38, pp. 61–67, 2005.
- [9] Strater, K., Richter, H. "Examining privacy and disclosure in a social networking community;" In: SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security, pp. 157–158, ACM, New York, NY, USA, 2007.
- [10] Tootoonchian, A., Gollu, K.K., Saroiu, S., Ganjali, Y., Wolman, A. "Lockr: social access control for web 2.0;" In WOSP '08: Proceedings of the first workshop on Online social networks, pp. 43–48. ACM, New York, NY, USA, 2008.
- [11] Marco Vanetti, Elisabetta Binaghi, Elena Ferrari, Barbara Carminati, and Moreno Carullo, "A System to Filter Unwanted Messages from OSN User Walls," IEEE transactions on knowledge and data engineering, vol. 25, no. 2, pp.285-297, February 2013.
- [12] J. Moody and C. Darken, "Fast Learning in Networks of Locally- Tuned Processing Units," Neural Computation, vol. 1, no. 2, pp. 281-294, 1989.
- [13] M.J.D. Powell, "Radial Basis Functions for Multivariable Interpolation: A Review," Algorithms for Approximation, pp. 143-167, Clarendon Press, 1987.
- [14] E.J. Hartman, J.D. Keeler, and J.M. Kowalski, "Layered Neural Networks with Gaussian Hidden Units as Universal Approximations," Neural Computation, vol. 2, pp. 210-215, 1990.
- [15] J. Park and I.W. Sandberg, "Approximation and Radial-Basis- Function Networks," Neural Computation, vol. 5, pp. 305-316, 1993.
- [16] A.K. Jain, R.P.W. Duin, and J. Mao, "Statistical Pattern Recognition: A Review," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp. 4-37, Jan. 2000.