International Journal for Modern Trends in Science and Technology
Volume: 03, Special Issue No: 02, March 2017
ISSN: 2455-3778
http://www.ijmtst.com

A Rule Based Message Filtering From OSN User Walls

Ch.Padma[1] | A.Shivani[2] | K.Haritha[3] | M.Nagavamsi[4]

[1,2,3,4]Department of IT, Andhra Loyola Institute of Engineering & Technology, Vijayawada, Andhra Pradesh, India.

To Cite this Article
Ch.Padma, A.Shivani, K.Haritha and M.Nagavamsi, "A Rule Based Message Filtering From OSN User Walls", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Special Issue 02, 2017, pp. 57-63.

ABSTRACT

One basic issue in today On-line Social Networks (OSNs) it gives users, the ability to control the messages posted on their own private space to avoid that undesired content or messages is displayed on their private wall. Up to now OSNs we provide little support to this requirement. now to fill this gap, we propose a system allowing OSN users to have a direct control on the messages posted on their walls. Proposed system is achieved through a flexible rule-based system, that 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.

I. INTRODUCTION

According to our facebook application,in be around average users creates 90 pieces of data deal for each month, while more than 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) are combined shared per each month. The vast and active character of these data creates the idea for the employment of web content mining strategies aimed toimpulsively discover informative or needed information inoperative within the data.They are contributory to provide an smartly maintain in difficult and sophisticated tasks intricate in OSN management, such as for instance occurance way in control or information filtering. Information filtering in OSN's has been greatly covered for what dealing textual documents and, more recently, web content . However, the purpose or intention of the majority of these suggestions is mainly to present clients or users a classification mechanism to pass up they are overcome by unwanted data. In OSNs, information filtering can also be used for a different, more sensitive, purpose. This is expected to the detail fact that are present in OSNs there is a chance of posting or commenting other posts on particular public/private areas, called in general walls. Information filtering can be used to provide users the capability to automatically control the messages written or displayed on their own user walls, by filtering out unwanted messages.Here we believe that, since so far we dint provide any key to avoid the unwanted messages. Todays OSN's provides a little support to control unwanted messages on user walls. For example, Generally 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, we are not having any content-based preferences are supported, therefore it is difficult prevent undesired messages, such as political or vulgar ones,illegal videos ,pictures, no matter of the user who posts them.By 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 confines since short texts do not provide sufficient word rates.

The work is to propose and experimentally evaluate an automated system, called Filtered Wall (FW),this able to filter undesired messages from OSN user walls.In this We exploit an automatic techniques such as Machine Learning (ML) text categorization techniques which is used assign an automatically filtering with each short text message a set of categories based on its content.

The major efforts in constructing a robust short text classifier are concentrated with a set of characterizing in the extraction and selection, discriminant features. The investigated solutions in this paper are an extension of those adopted in a previous work by us from which we acquire the learning model and the elicitation procedure for generating pre-classified data. The original set of features, derived from internal properties of short texts, is enlarged here including external 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. 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.

In neural model we have two level hierarchical classification strategy. In the first level, the RBFN categorizes short messages as Neutral and Non-Neutral. In the second stage, Non-Neutral messages are classified producing gradual estimates of appropriateness to each of the considered category.

It is a a flexible language to specify Filtering Rules (FRs), by which users can state what contents should not be displayed on their walls BlackLists (BLs), that is, lists of users that are temporarily prevented to post any kind of messages on a user wall.

. The best part of our knowledge that the proposal of a system is automatically filter undesired messages from OSN user walls on both the basis message content and the message creator relationships and characteristics. The current paper substantially extends 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 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.

It describes the ML-based text classification method used to categorize text contents, whereas Section illustrates FRs and BLs. Section we illustrates the evaluation and performance of the proposed system, whereas the prototype application is described.

II. RELATED WORK

In this paper we contribution the design of a system providing customizable content-base message filtering for OSNs, based on ML techniques. As we have pointed out in the introduction, In this we are the first proposing such kind of application for OSNs. However, our work has relationships both with the state of the art in content-based filtering, as well as with field of policy-based personalization for OSNs and, more in general, web contents.

2.1 Content-based filtering

In an alternate way an information producer and present to the user those information that are likely to satisfy his/her requirements.

In content-based filtering each user is assumed to operate independently. As a result, a content-based filtering system selects information items based on the correlation between the content of the items and the user preferences as opposed to a collaborative filtering system that chooses items based on the correlation between people with similar preferences.. Documents processed in content-based filtering are mostly textual in nature and this makes content-based filtering close to text classification. The activity of filtering can be modelled More complex filtering systems include multi-label text categorization automatically labeling messages into partial thematic categories.

ML can be done by using content-based filtering paradigm according to which a classifier is automatically induced by learning from a set of pre-classified examples. A remarkable variety of related work has recently appeared, which differ for the adopted feature extraction methods,

The application of content-based filtering on messages posted on OSN user walls poses additional challenges given the short length of these messages other than the wide range of topics

that can be discussed. Short text classification has received up to now few attention in the scientific community. Recent work highlights difficulties in defining robust features, essentially due to the fact that the description of the short text is concise, with many misspellings, non standard terms and noise. In our scenario, we consider a key feature to define the flexible policy-based personalization strategies.

2.2 Policy-based personalization of OSN contents

We classification, the method to proposed the categorize of short text messages in order to avoid undesired message overflow. The system described in focuses on Twitter2 and associates a set of categories with each tweet describing its content. In our filtering policy language allows the setting of FRs according to a variety of criteria, that do not consider only the results of the classification process but also the relationships of the wall owner with other OSN users as well as information on the user profile. Moreover, our system is complemented by a flexible mechanism for BL management that provides a further opportunity of customization to the filtering procedure.

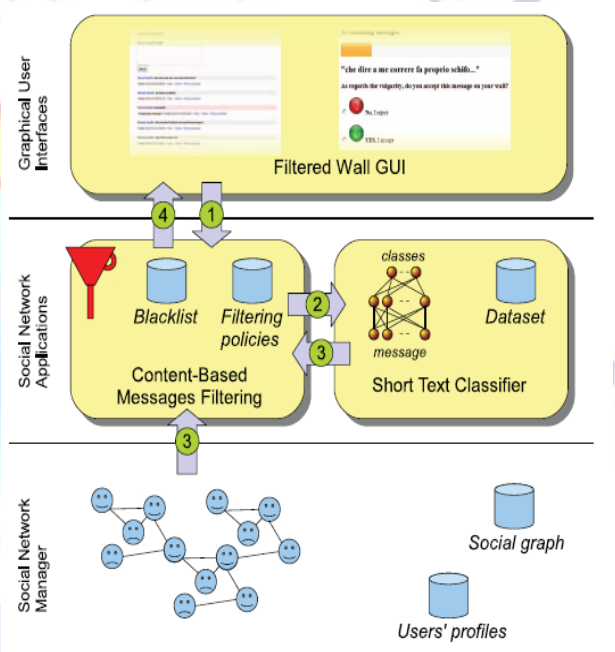
We have different criteria for filtering policy such as follows:

1) rate resources with respect to four criteria: trustworthiness, vendor reliability, privacy, and child safety

2) In particular, it supports filtering criteria which are far less flexible than the ones of Filtered Wall since they are only based on the four above-mentioned criteria. Moreover, no automatic classification mechanism is provided to the end user.

since it can be consider both to protect objects from unauthorized subjects to extension of access control, and subjects from inappropriate objects. In the field of OSNs, the majority of access control models proposed so far enforce topology-based access control, according to which access control requirements are expressed in terms of relationships that the requester should have with the resource owner. We use a similar idea to identify the users to which a FR applies. However, filtering policy language extends the languages proposed for access control policy specification in OSNs to cope with the extended requirements of the filtering domain. Indeed, since we are dealing with filtering of unwanted contents rather than with access control, one of the key ingredients of our system is the availability of a description for the message contents to be exploited by the filtering mechanism. In this, no one of the access control models previously cited exploit the content of the resources to enforce access control. Moreover, BL's will maintain the access control models.

Finally, we have a relationships with the policy frameworks and policy language which have been so far proposed to support the specification and enforcement of policies expressed in terms of constraints on the machine understandable resource descriptions provided by Semantic However, although the frameworks are very powerful and general enough to be customized and/or extended for different application scenarios they have not been specifically conceived to address information filtering in OSNs and therefore to consider the user social graph in the policy specification process.



III. FILTERED WALL ARCHITECTURE

This is the architecture in support of OSN services , which represent the three-tier structure . The first layer is called Social Network Manager (SNM) which commonly aims to provide the basic OSN functionalities (i.e., profile and relationship management), whereas the second layer provides the support for external Social Network Applications (SNAs).4 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. 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. The strategy underlying this module is described in Section IV. In contrast, the first component exploits the message categorization provided by the STC module to enforce the FRs specified by the user. BLs can also be used to enhance the filtering process (see Section V for more details). As graphically depicted in Figure 1, the path followed by a message, from its writing to the possible final publication can be summarized as follows:

1) After entering the private wall of one of his/her contacts, the user tries to post a message, which is intercepted by FW.

2) ML-based text classifier extracts metadata from the content of the message.

3) FW uses metadata provided by the classifier, together with data extracted from the social graph and users' profiles, to enforce the filtering and BL rules.

4) Depending on the result of the previous step, the message will be published or filtered by FW. In what follows, we explain in more details some of the above-mentioned steps.

IV. SHORT TEXT CLASSIFIER

Established techniques used for text classification work well on datasets with large documents such as newswires corpora, but suffer when the documents in the corpus are short. In this context, critical aspects are the definition of a set of characterizing and discriminant features allowing the representation of underlying concepts and the collection of a complete and consistent set of supervised examples. Our study is aimed at designing and evaluating various representation techniques in combination with a neural learning strategy to semantically categorize short texts. From a ML point of view, we approach the task by defining a hierarchical two level strategy assuming that it is better to identify and eliminate "neutral" sentences, then classify "non neutral" sentences by the class of interest instead of doing everything in one step. This choice is motivated by related work showing advantages in classifying text and/or short texts using a hierarchical strategy.The first level task is conceived as a hard classification in which short texts are labelled with crisp Neutral and Non-Neutral labels. The second level soft classifier acts on the crisp set of non-neutral short texts and, for each of them, it is "simply" produces estimated to the appropriateness or "gradual membership" for each of the conceived classes, without taking any "hard" decision on any of them. Such a list of grades is then used by the subsequent phases of the filtering process.

4.1. Text Representation

In a given document we extract an appropriate set of features it represents a crucial task strongly affecting the performance of the overall classification strategy..For text categorization we proposed different sets of features in the literature ,however the most appropriate feature set and feature representation for short text messages have not yet been sufficiently investigated. Proceeding from these considerations and on the basis of our experience, we consider three types of features, BOW, Document properties and Contextual Features (CF). The first two types of features, already used in, are endogenous, that is, they are entirely derived from the information contained within the text of the message. Text representation using internal knowledge has a good general applicability, however in operational settings it is conforming to use also external knowledge, i.e.,from outside the message body any source of information directly or indirectly related to the message itself. We introduce CF modeling information that characterize the environment where the user is posting. These features play a key role in deterministically understanding the semantics of the messages .

4.2 Machine Learning-based Classification

We introduce a two level classification process hierarchical short text categorization. The first-level classifier performs a binary hard categorization that labels messages as Neutral and Non-Neutral. The first-level filtering task facilitates the subsequent second-level task in which a finer-grained classification is performed.

The second-level classifier performs a soft-partition of Non-neutral messages assigning a given message a gradual membership to each of the non neutral classes.

The pre-classified collects a messages presents some critical aspects greatly affecting the performance of the overall classification strategy. ML-based classifier needs to be trained with a set of sufficiently complete and consistent pre-classified data. Here we have a difficulty of satisfying this

limitation is essentially related to the subjective character of the interpretation process with which an expert decides whether to classify a document under a given category.

V. FILTERING RULES AND BLACKLIST MANAGEMENT

In this section, we introduce the rule layer adopted for filtering unwanted messages. We start by describing FRs, then we illustrate the use of BLs. An filtering rule is applied to filter the unwanted messages and it maintain a blacklist management.

In what follows, we maintain a directed graph for 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 and, possibly, the corresponding trust level, which represents how much a given user considers trustworthy with respect to that specific kind of relationship the user with whom he/she is establishing the relationship. Without loss of generality, let us consider that trust levels are rational numbers in the range. There exists a direct relationship with two users in a given type RT and trust value X , if an edge of trust are placed in direct computation for indirect relationships, we proposed many algorithms in the literature that can be used in our scenario as. Such algorithms mainly differ on the criteria to select the paths on which trust computation should be based, when many paths of the same type exist between two users.

5.1 Filtering rules

In filtering rules we consider three main issues that, should affect a message filtering decision. First of all, in OSNs like in everyday life, the same message may have different meanings and relevance based on who writes it. As a consequence, FRs allow the creators to create limitation on who message creators. Creators on which a FR applies can be selected on the basis of several different criteria, in this we follow different criteria for allowing filtering rules 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.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. All these options are formalized by the notion of creator specification, defined as follows.

Definition 1. Creator specification).

A creator specification creator Spec implicitly denotes a set of OSN users. Itcan have one of the following forms, possibly combined:

1) a set of attribute constraints of the form an OP where an is a user profile attribute ne, 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 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 tomaxTrust.

Definition 2. (Filtering rule).

A filtering rule FR is a tuple 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 contentconstraints 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 tomake the constraint satisfied;

_ action 2 fblock; notifyg denotes the action to be performed by the system on the messages matching contentSpec and created by users identified by creatorSpec.

In general, the same user will apply more filtering rule .The messages can only send when the user is not in blocked state.By using the filtering rules we are maintain a alert message for the user blocking/unblocking.In this we maintain different criteria, It may happen that a user profile does not contain a value for the attribute(s)referred by a FR In that case, the system is not able to evaluate whether the user profile matches the FR. Since how to deal with such messages depend on the considered scenario and the wall owner attitudes, we ask the wall owner to decide whether to block or notify messages originating from a user whose profile does not match against the wall owner FRs because of missing attributes.

5.2 Online setup assistant for FRs

We address the problem of setting thresholds to filter rules, by conceiving and implementing within FW, an Online Setup Assistant (OSA) procedure.It maintain a database with OSA presents by using

that the user with a set of messages selected from the dataset discussed in Section .It is a user decision form whether to accept or reject the messages For each message, the user tells the system the decision to accept or reject the message. The collection and processing of user decisions on an adequate set of messages distributed over all the classes allows to compute customized thresholds representing the user attitude in accepting or rejecting certain contents.

Messages are selected according to the following process. A certain amount of non neutral messages taken from a fraction of the dataset and not belonging to the training/test sets, are classified by the ML in order to have, for each message, the second level class membership values.

5.3 Blacklists

A further component in our proposed system is a BL mechanism, which is used to avoid messages from undesired creators, which independent from their contents. BLs are directly managed by the system, which are able to determine who are the users to be placed in the BL and decide when users retention in the BL is finished. It has flexible which is used to enhance flexibility, such information are given to the system through a set of rules, hereafter called BL rules. Such rules are not defined by the SNM, therefore they are not meant as general high level directives to be applied to the whole community. Rather, we decide to let the users themselves .Only authourized persons have ability to send or receive messages from the user walls. Both FRs and BLs will main the data.

Similar to FRs, our BL rules make the wall authourized persons able to identify users to be blocked according to their profiles as well as their relationships in the OSN. Therefore, by means of a BL rule, wall owners are for example able to ban from their walls users they do not directly . This banning will maintain a time period for each use.Moreover, banning criteria may also take into account users' behavior in the OSN. More precisely, among possible information denoting users' bad behaviour we have focused on two main measures. The first is related to the principle that if within a given time interval a user has been inserted into a BL for several times, say greater than a given threshold, he/she might deserve to stay in the BL for another while, as his/her behavior is not improved. This principle works for those users that have been already inserted in the considered BL at least one time. In contrast, to catch new bad behaviors, we use the Relative Frequency (RF) that let the system be able to detect those users whose messages continue to fail the FRs. The two measures can be computed either locally, that is, by considering only the messages and/or the BL of the user specifying the BL rule or globally, that is, by considering all OSN users walls and/or BLs.

VI. CONCLUSION

Moreover till now we are aware that a usable GUI could not be enough, representing only the first step. Indeed, the proposed system may suffer of problems similar to those encountered in the specification of OSN privacy settings. In this context, many empirical studies have shown that average OSN users have difficulties in understanding also the simple privacy settings provided by today OSNs. To overcome this problem, a promising trend is to exploit data mining techniques to infer the best privacy preferences to suggest to OSN users, on the basis of the available social network data . As future work, we intend to exploit similar techniques to infer BL rules and FRs. Additionally, we plan to study strategies and techniques limiting the inferences that a user can do on the enforced filtering rules with the aim of bypassing the filtering system, such as for instance randomly notifying a message that should instead be blocked, or detecting modifications to profile attributes that have been made for the only purpose of defeating the filtering system.

REFERENCES

[1] A. Adomavicius, G.and Tuzhilin, "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible xtensions," 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.