A SYSTEM TO FILTER OSN USERWALLS

Navin Raj

Introduction

This main project entitled "**A SYSTEM TO FILTER OSN USERWALLS"** is a web-based service that allows individuals to construct a public or semi-public profile within the service, Articulate a list of other users with whom they share a connection and View and traverse their list of connections and those made by others within the service.

The main goal of the system is to design an online message filtering system that is deployed at the OSN service provider side. Once deployed, it inspects every message before rendering the message to the intended recipients and makes immediate decision on whether or not the message under inspection should be dropped. 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. First the message is filtered with filtering rules.

Filtering rules (FR) give the result of ML categorization process, which filter the user wall and relationship of user. Further Blacklist is also supported by the system, it can be said as users who post the unwanted message will be kept in blacklist for particular period of time. By using this rule, OSN is provided with more security.

Today OSNs provide very little support to prevent unwanted messages on user walls. For example, Face book 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.

This project contains six modules

- Admin
- Users
- Filtering Rules
- Online setup assistant for FR thresholds

- Blacklist
- PGRP

3.3 MODULE DESCRIPTION

1.Admin

1.1 Defining and maintaining FRs specification

1.2 Monitoring Blacklist

1.3 Monitoring Spammers and Deactivating account

1.4 View User List

2.Users

2.1 Account Creation in OSN

2.2 Sign In To OSN

2.3 Sending Friend Request

2.4 Accepting Friend Request

2.5 Adding Post

2.6 Sharing Post

2.7 Performing Online Setup Assistant(OSA) procedure

After the Preprocessing performed on added Post, Filtering Rules are calculated as mentioned below, and then percentage of restricted illegal bad are calculated. Further Trust Value Calculations are done. Then for each message, the user tells the system the decision to accept or reject the message.

2.8 Placing the users to Black List

From user side:

- If the user finds any misbehavior then Black List plays its role from user side

From system side:

- After evaluating BL Rules, the sender is automatically inserted to Black List

2.9 Withdrawing the users from Blak List if needed

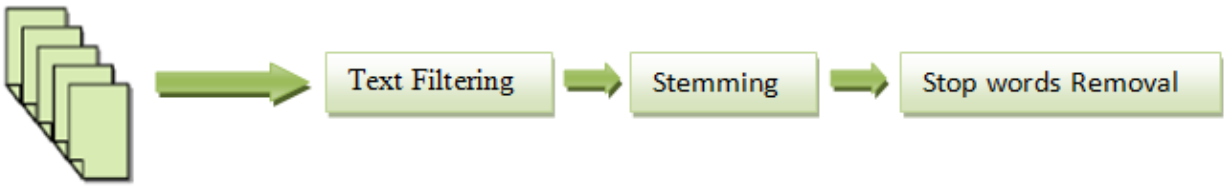
2.10 Reporting Spammers

2.11 Searching Friend

3. Filtering Rules

In defining the language for FRs specification, we consider three main issues that, in our opinion, 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 should allow 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. Given the social network scenario, 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

Algorithm Preprocessing



Text filtering**:** In the text filtering step, all terms that are useless or would introduce noise in filtering process are removed from the input message. Among such terms are:

- HTML tags (e.g. <table>) and entities (e.g. &) if any.
- non-letter characters such as "$", "%" or "#" (except white spaces and sentence markers such as '.', '?' or '!') Note that at this stage the stop-words are not removed from the input.

Stemming **:** Stemming algorithms are used to transform the words in texts into their grammatical root form, and are mainly used to improve the Information Retrieval System's efficiency. To stem a word is to reduce it to a more general form, possibly its root. For example, stemming the term interesting may produce the term interest. Though the stem of a word might not be its root, we want all words that have the same stem to have the same root.

Elimination of Stop Words **:** After stemming it is necessary to remove unwanted words. There are 400 to 500 types of stop words such as ―of‖, ―and‖, ―the,‖ etc., that provide no useful information about the message. Stop-word removal is the process of removing these words.

Filtering Rules are customizable by the user. User can have authority to decide what contents should be blocked or displayed on his wall by using Filtering rules. For specify a Filtering rules user profile as well as user social relationship will be considered. FR= {Trustier, SOUs, Rule, TuV}

Trust Value Calculations

- Positive with content (PC)
- Positive without content (PWC)
- Negative with content (NC)
- Negative without content (NWC)

Porter Stemmer Algorithm

At the very basics of it, the major difference between the porter and lancaster stemming algorithms is that the porter stemmer is less aggressive than lancaster.

The three major stemming algorithms are Porter, Snowball(Porter2), and Lancaster with the aggressiveness continuum basically following along those same lines. Porter is the least aggressive algorithm.

Porter: Most commonly used stemmer without a doubt, also one of the most gentle stemmers. It is also the oldest stemming algorithm by a large margin.

Porter2: Regarded as an improvement over porter, and for good reason. Its computation time is slightly faster than porter.

Lancaster: Very aggressive stemming algorithm, sometimes to a fault. With porter and snowball, the stemmed representations are usually fairly intuitive to a reader, not so with Lancaster, as many shorter words will become totally obscure and confusing.

Snowball is actually a language designed by Martin Porter for the precise definition of stemmers, it is not itself a stemmer. The algorithm you refer to is known as "English Stemmer" or "Porter2 Stemmer". It is very similar to "Porter Stemmer" but with slightly improved rules.

4.Online setup assistant for FRs threshold

In here address the problem of setting thresholds to filter rules, by conceiving and implementing within FW, an Online Setup Assistant (OSA) procedure. OSA presents the user with a set of messages selected from the dataset discussed in Section . 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 computing customized thresholds representing the user attitude in accepting or rejecting certain contents. Such 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.BlackList

A further component of our system is a blacklist mechanism to avoid messages from undesired creators, independent from their contents. Blacklist are directly managed by the system, which should be able to determine who are the users to be inserted in the blacklist and decide when users retention in the blacklist is finished. To enhance flexibility, such informationare given to the system through a set of rules. Rather, we decide to let the users themselves, i.e., the wall's owners to specify blacklist rules regulating who has to be banned from their walls and for how long. Therefore, a user might be banned from a wall, by, at the same time, being able to post in other walls. Blacklist are directly managed by the system. This should be able to determine the users to be inserted in the BL and decide when to retain user back from the blacklist. To enhance flexibility, such information is given to the system through a set of rules.

BL rules: INPUT = {Sender, FB, TuV, ThV} Where

- Sender is the OSN user who is sending the message;
- FB is the FeedBack gain by the sender after sending the message
- TuV is the new Trust Value calculated as formulas
- ThV is the Threshold Value.

6. PASSWORD GUESSING RESISTANT PROTOCOL (PGRP)

Password Guessing Resistant Protocol (PGRP), derived upon revisiting prior proposals designed to restrict attacks. While PGRP limits the total number of login attempts from unknown remote hosts to as low as a single attempt per username, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an attack. PGRP uses either IP addresses, cookies, or both to identify machines from which users have been successfully authenticated.

SYSTEM STUDY

EXISTING SYSTEM

Todays OSNs provide very little support to prevent unwanted messages on user walls. For example, Face book 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.

PROPOSED SYSTEM

In this paper we propose a technique known as filtered wall (FW), which is used for filtering unwanted messages. The Filtered Wall scans each message before being posted on wall. Filtering rules are used to determine which contents should be allowed on user's wall and which messages should be blocked. Further it will also provide a Blacklisting mechanism. Blacklist will

be an automated mechanism which will block users posting undesired messages on the user walls. The prohibition can be approved for uncertain period of time.

CONCLUSION

Inspecting the messages posted on OSN user walls is important issue in today's world.Our proposed system uses an automated mechanism to scan the messages before being posted on the user's wall and further filters those messages from OSN user walls which are unwanted and undesired. We have also proposed automated blacklist mechanism which blocks the users who repeatedly try to post such undesired messages ignoring the given warnings.Hence, our proposed system provide more security to OSN user walls and there for no objectional content canbe circulated through our proposed mechanism for OSN user walls.

SCOPE FOR FUTURE ENHANCEMENT

Every application has its own merits and demerits. The project has covered almost all the requirements. Further requirements and improvements can easily be done since the coding is mainly structured or modular in nature. Future Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving to the user, confidence that the new system will work and be effective. Changing the existing modules or adding new modules can append improvements. Future enhanced we can developed this application with video calling option and realtime chatting also we can add money transfer facility in between friends.

BIBLIOGRAPHY

The following books and websites were very helpful during the completion of project:

REFERENCES

- "Java The Complete Reference, 8th Edition", McGraw-Hill Osborne Media; 8 edition (June 22, 2011).
- "Tomcat: The Definitive Guide", Jason Brittain (Author), Ian F. Darwin (Author), O'Reilly Media; Second Edition (October 30, 2007).
- Robert Vieira, Professional Microsoft SQL Server 2008 Programming", Publisher: Wiley John & sons, Incorporated, 2009
- Richard Fairley, "Software Engineering Concept", Publisher: Tata McGraw- Hill Education, 2001
- Roger S Pressman, "Software Engineering: A Practitioner's Approach"(first edition),1982
- Roger S Pressman, "Software Engineering: A beginner's guide"(1988)

Websites:

- Codeguru, http://www.codeguru.com/
- Codeproject, http://www.codeproject.com/
- http://www.jpgtutorials.com/introduction-to-java-server-pages- jsp