AN ENHANCED PRIVACY RULE BASED MODEL FOR FILTERING UN-PREFERRED MESSAGES

N. Gomathivani,
Research scholar,
Govt. Arts College (Autonomous),
Salem-7,
n.gomathivani@gmail.com

Prof. K. Akilandeswari,
Associate Professor,
Department of Computer Science,
Govt. Arts College (Autonomous),
Salem-7,
akilamanivelan@gmail.com

ABSTRACT:

The online social networks (OSN) offers proficient message controls that are posted on their private space in order to avoid un-preferred content displayed to users. But, OSN provides a low supportive and flexibility to the private message in the user's own space. Most of the existing works on OSN presents a system to facilitate user by discarding the messages posted on their private wall. The existing works also develops flexible rule based system with the filtering criteria to post only useful messages on their walls for user satisfaction. The machine learning based classifier presents involuntarily labeling of messages that support content based filtering. Moreover, OSN filters the message content based on message originator relationship and characteristics. OSN offer the rule layer with classification module with the semantics for filtering policy to improve the domain.

The drawback of existing work is that filters did not concern about the user privacy demand. The provisions for the feedbacks on the online learning as well as the nomenclature of the users in the black list are not mentioned. Hence, the challenge lies in establishing better filtering technique. The proposed work is user privacy concerned social proximity rules to develop an efficient filter for open social network. Proximity rule estimation (PRE) provides private and verifiable proximity computation based on polynomial secure share. PRE address the user privacy concern by getting the feedback forms from the user for friend-like nomenclature. Proposed PRE is able to discover the potential friends with the preferred message exchange between them using relational privacy index. And also helps to identify a variety of possible attack messages by analyzing real traces. Additionally, PRE develops novel solution for secure proximity estimation and allows user to identify the acceptable messages that are listed in their social network space. Proposed work intends in fulfilling user privacy needs and demands in designing OSN filters. The adequate numbers are given for the privacy feedbacks on the online learning and the user nomenclature are exclusively inserted in the black list for classification of filter rules. Experimental evaluations are conducted to prove the better performance of PRE in terms of attack density, minimum execution time and less memory space utilized.

Keywords: Online social networks, information filtering, short text classification, polynomial secure share.

1. INTRODUCTION:

Online Social Networks allows the users to be division of a virtual community. Mainly well-suited for intermediate communication, share, and is also defined as a network of social interactions and personal relationships. The two widely used sites are Face book, Twitter, MySpace and so on. So, the websites grant users through easy tools to create a tradition profile with text and pictures. A characteristic profile includes essential information regarding the user, at least one photo and perhaps a blog or further comments published by the user. Replacement of more than few types of content, including free text, image, audios and video data impacts a communications regularly. Information filtering techniques maintains more sensitive communication. This is real fact, due to that the possibility of sharing or commenting other posts on particular public/private areas from OSNs general walls is preserved. The information filtering can be used to provide users capability to routinely control the messages written on their individual walls, by filtering un-preferred messages.

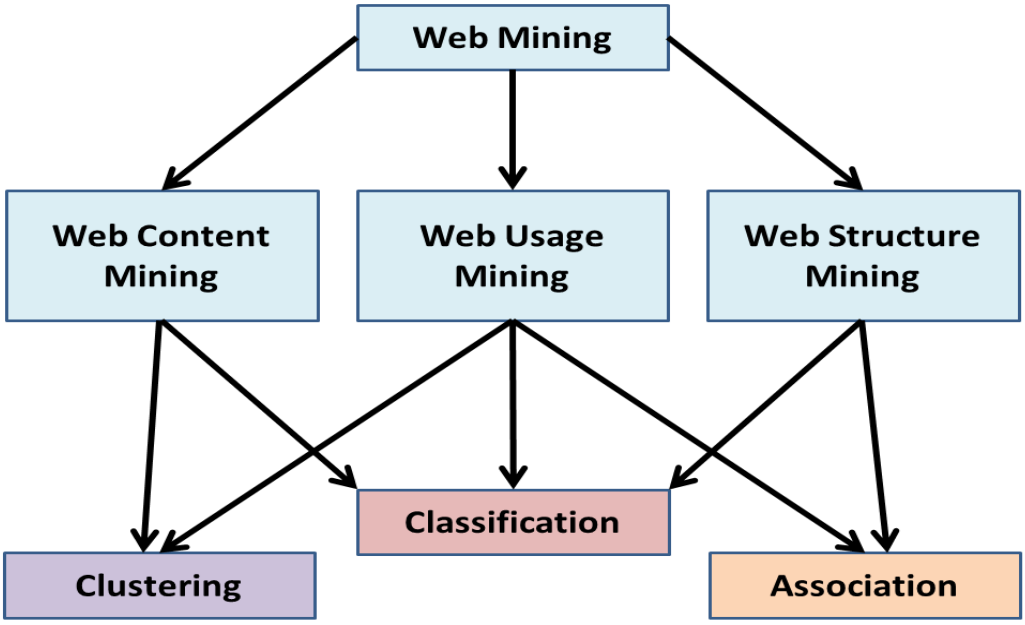

Fig 1: Web Mining

Web based content mining techniques are offered with the service of not only using earlier substances but also involves different classification, clustering and association strategies facilitating various web related applications.

The main challenge of OSNs lies in offering security to private messages and resolve privacy issues in order to enhance central server trustworthiness. As most servers share the information privately, the negative consequences are more. Finally, we consider the attack of potential messages and estimate the proximity rules, how to recognize the problem in one's objective locality. The main idea of proximity measure contains the predictive friendship approach involving in social networks. This work details the technique top protect private messages on social network using polynomial secure share.

2. LITERATURE REVIEW:

The author in [1] avoids difficulty more possibly and error-prone characteristics build using a learning method that operates sensibly well without preliminary characteristics engineering. This work, involves prediction by partial matching (PPM) method that compresses the text contents to capture text features with the generation of language model to a specific text. And also researchers demonstrate that the method provided a large precision of text classification and container be worn as an option to state-of-art learning algorithms. However, the work fails in handling multi-labeled texts, particularly medical texts when multiple classifications of strange documents is seen and also requires a set of domain accurate features extraction from the text.

In this paper [2], author addressed the problem faced in the micro blogging services such as Twitter, on classifying the short text messages with raw data. The short texts do not provide adequate word occurrences; conventional classification methods based on "Bag-Of-Words" have restrictions. The proposed work uses a minimum set of domain-specific features collected from the users profile and text. The proposed approach efficiently classifies the text to a preprocess group of standard classes such as News, Events, Opinions, Deals, and Private Messages. In future work, a competent URL hierarchy to gain more reasoned set of Web pages and evaluation and permutation of the proposed approach with dynamic pruning approaches.

In this paper [3], Web search engines typically index and retrieve at the page level. This work also investigate a dynamic pruning strategy that allows the query processor to first determine the most promising websites and then precede with the similarity computations for those pages only within these sites. In future work text based communication on web page is included to increase the effectiveness of the search engines.

In this paper [4], the author**s** reports on a study of text-based communication based on Web-based groupware system, DHS. Since, the system does not support the threading message, so more awareness is required to investigate how participants use the referential space to connect to each other's contributions. In order to improve the functioning of system more reliable, the work in [4] incorporates two main approaches of trust annotations is included in the web page. This will give more feasibility to the web based system.

In [5], a two level approach is developed to merge trust, provenance, and annotations in Semantic Web systems. And also describe an algorithm for gathering privacy relationships using provenance information and trust annotations in Semantic Web-based social networks. In future work by addressing security of semantic web pages and also include digital signatures to improve the security for semantic web services.

Most of the security related issues in semantic **w**eb services is illustrated in [6]. It is described to declaratively in OWL-S based on ontologies annotations. The ontolology annotation provides the OWL-S input and output parameters. Even the encryption process involves a set of security metrics based on their digital signatures. Additionally, to incorporate the policies concentrates for privacy authentications into OWL-S investigation and activist profiles. This work extends to encryption process based on the signing messages replace between requester and provider. Future work will address negotiation protocols. More complex policies that address combinations of these security notions and other user-defined policies will be subject of future work.

In this paper [7], Short messages frequently consist of only a little word, and therefore provided a brave to usual bag-of-words based on spam filters. By three corpora of short messages and message field consequent from actual SMS, blog, and spam messages, they estimate feature-based and compression-model-based spam filters. They survey to facilitate the bag-of-words filters preserve better considerably using various different features, though compression-model filters perform quite well as-is. They fulfill that content filtering for short messages is considerably efficient. In future, easy to personality spam filters can be shared and this will be more efficient and feasible.

In this paper [8], they show that a set of separately developed spam filters may be mutual in easy way to provide considerably better filtering than any of the personality filters. The results of fifty-three spam filters performed at the TREC 2005 Spam Track are shared post-hoc so as to imitate the comparable on-line operation of the filters. The stacking methods show to provide more development, but only for very huge corpora. Of the stacking methods, logistic regression yields the recovered result. Finally, they show that it is potential to choice a priori small subsets of the filters that, when combined, still outperform the best individual filter by a considerably margin. To increase the probable value for user appropriate feedback, for future strengthening to learn is incorporated for the web pages.

In this paper [9], to increase the document filtering deployed based on the web environments and reduces to the information overload of users. They originate online information filtering as a reinforcement learning problem, i.e. TD (0). This “learning by observation” advance is contrasted with predictable consequence feedback methods which involve the precise user feedbacks. Field tests have been performed which complex 10 users analysis an overall of 18,750 HTML papers through 45 days. For future work flexible rule based system which allows to improvement the filtering criteria using content based filtering.

In this paper [10], Online Social Networks (OSNs) is to grant users the facility to manage the messages posted on their own private space to avoid that un-preferred content is displayed. Up till now, OSNs afford small support to this requirement. To fulfill the problem, to allow the system have an instantly control on the messages posted on their walls from OSN users. This work concentrated on Content-based filtering and Policy-based personalization of OSN contents for filtering un-preferred messages. The policy-based filter based on classification method to exploit the use of filtering policy to decide on how and when to filter un-preferred information. For future work, to plan address the problems of user privacy concern to the rule based content filtering by investigating the use of online learning paradigms able to include label feedbacks from users.

3. PROPOSED WORK:

“An enhanced proximity rule-based estimation (PRE) for user privacy” mainly concentrates on message filtering based on polynomial secure share techniques. The proposed PRE works on three major phases as follows:

- User Privacy Feedback List.
- Discovery of Possible Attack Messages.
- Proximity Rule Estimation with Relational Index.

3.1 User Privacy Feedback List

User’s privacy feedback lists are generated from their social media activity and their presence. To enlarge or virtual ID using to the users declared on announce and social coordinates. The users tracking based on their digital signature for authentication to avoid durable link facility. Mobile users to realize and cooperates with friends in physical locality from Mobile social networks.

Mobile social network is grand to promise for enabling many exciting new applications to support serious privacy and security concerns. Generally, users are unwilling to reveal their private messages and personal profile to an unknown person in their vicinity. The trust information is an arbitrary person on blindly un-wised.

3.2 Discovery of Possible Attack Messages:

The feedback list of user privacy recognizes a variety of possible attack messages against friend detection by evaluating the actual traces. To distinguish the curious regarding other users own and location information resolve try their greatest, to extract the information and detect from all messages. The number of possible attack messages launched to the role of user location privacy more than real traces will be occurred.

A variety of possible attack messages against proximity computation based on social coordinates evaluate the efficiency of true traces. In order to recognize the possible attack messages compute the social proximity. The estimation of proximity provides secure share increasing the privacy of users. Based on the data mining techniques the best privacy preference increases to hint from OSNs.

3.3 Proximity Rule Estimation with Relational Index:

This problem contains the solution of proximity rule estimation with relational index for possible attack messages. Proximity filters allows users to fast filter away users improbable to turn into friends does not check a rival from forging social coordinates concluding proximity effect. Proximity rule estimation provides private and verifiable proximity computation based on polynomial secure share (PSS). Finally, to verify the proximity rule based on their social co ordinates proximity result.

Proximity rule estimation determines proximity that exceeds the threshold. Polynomial secure share effective solution to privacy-preserving computation allows certain algebraic operations on different types to be performed using (possibly different) algebraic operations directly on process. The below algorithm elaborates the proposed techniques with polynomial secure share steps as follows:

3.4. Polynomial Secure Share steps:

1. The basic scheme if we set $Fi(xj) = ri\ jr\_i\ j\ fi(xj)$, then the result will be 0 if $xj \in I1,i$, otherwise be a random number.
2. In order to obtain the number of matching attributes ($m1,i$), one way is to employ the equality test protocol based on PSS, which tests whether each shared secret $Fi(xj)$ equals to 0 or not, and the output is 0 or 1 which is still shared among the parties.
3. However, the equality test protocol incurs too high communication cost.
4. We adopt a blind-and-permute (BP) method to obliviously permute $P1$'s shares of each $Fi(xj)$, so that the linkage between $Fi(xj)$ and its corresponding attribute xj is broken.
5. A BP protocol between two parties A and B where each data item (e.g., $Fi(xj)$) is additively split between them is described in.
6. A encrypts each of its shares using additive homomorphic encryption and sends to B.
7. B then generates a different random number $r\ j$ for each shared item, and randomizes each of A's shares by adding $r\ j$, while subtracting $r\ j$ for its own corresponding shares.
8. B randomly permutes the randomized shares, and sends back to A.
9. All the computations are done over the cipher texts.

4. RESULT AND DISCUSSIONS:

In this section evaluate performance An Enhanced privacy concerned Social Proximity Rules to Filters Un-Preferred Messages through java with weka environment. To confirm the analytical results, we implemented Social Proximity Rules to Filters Un-Preferred Messages techniques in java environment and evaluated the Social Proximity Rules performance of technique. The performance of is evaluated by the following metrics.

- Attack density
- Execution time for proximity rule estimation
- Memory space required to generate proximity rules.

4.1. Attack Density

Attack density is defined as the rate of attacking in terms of encountering the anomalous activity like un-preferred message post in user's private wall causing a problem.

Table: 4.1. Attack density

No. of users	Attack density (%)	
	OSN (Existing)	PRE (Proposed)
10	65	58
20	68	62
30	70	68
40	75	70

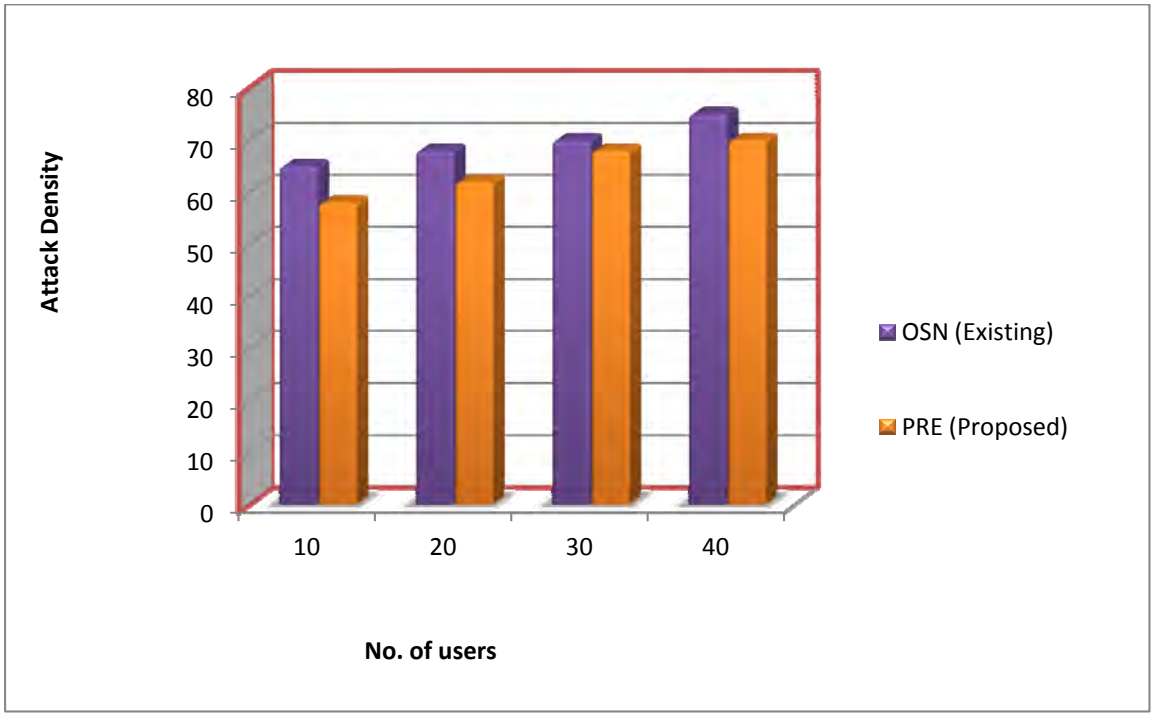

Fig: 4.1. No. of users Vs Attack Density

Figure 4.1 demonstrates Attack Density. X axis represents the number of users whereas Y axis denotes Attack Density per users using both the existing open social network filtering (OSN) and Proximity Rule Estimation (PRE).When the users increased, Attack density gets decreases accordingly. Figure 4.1.shows better performance of Proximity Rule Estimation (PRE) scheme in terms of users than existing open social network filtering (OSN). Proximity Rule Estimation (PRE) achieves 10 to 15% higher attack density of user variation when compared to existing system.

4.2. Execution time for proximity rule estimation

Time taken to estimate the proximity rule on detection of un-preferred message is defined as execution time.

Table: 4.2. Execution time for proximity rule estimation

No. of users	Execution time (Seconds)	
	OSN (Existing)	PRE (PRO)
10	0.024	0.018
20	0.036	0.024
30	0.042	0.034
40	0.054	0.045

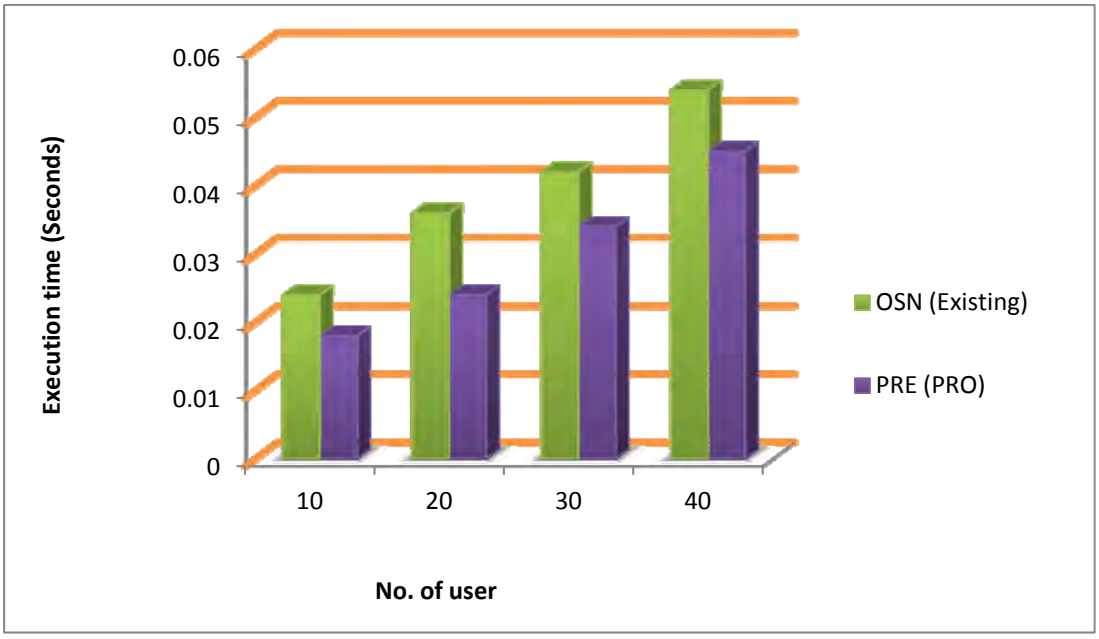

Fig: 4.2. No of users Vs Execution Time

Figure 4.2 demonstrates execution time with respect to number of users. X axis represents the number of users whereas Y axis denotes Execution Time per users using both the existing open social network filtering (OSN) and Proximity Rule Estimation (PRE).When the users increased, Execution Time gets decreases accordingly. Figure 4.2.shows better performance of Proximity Rule Estimation (PRE) scheme in terms of users than existing open social network filtering (OSN). Proximity Rule Estimation (PRE) achieves 15 to 25% less Execution Time of user variation when compared to existing system.

4.3. Memory space required to generate proximity rules

Forecast the memory space required by PRE to estimate proximity rules on prevention of un-preferred message.

Table: 4.3. Memory Space required on estimation of proximity rule

No. of users	Memory space (MB)	
	OSN(Existing)	PRE(PRO)
10	27.34	25.98
20	33.90	31.09
30	35.78	33.65
40	38.87	36.90

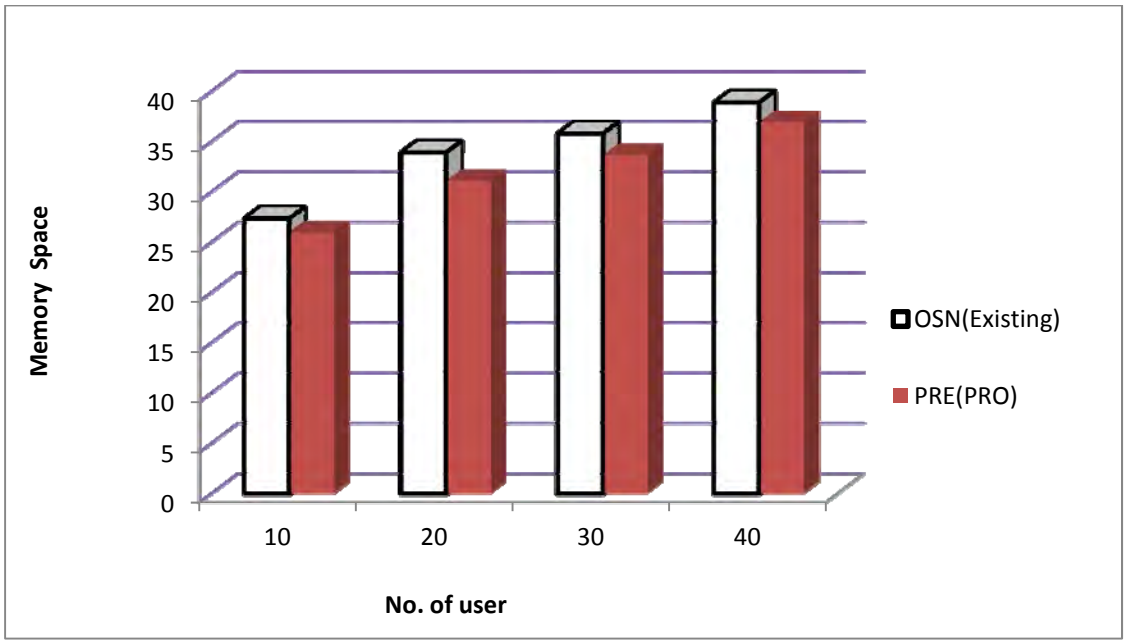

Fig: 4.3. No. of users Vs Memory space

Figure 4.3 demonstrates Memory space. X axis represents the number of users whereas Y axis denotes Memory space per users using both the existing open social network filtering (OSN) and Proximity Rule Estimation (PRE).When the users increased, Memory space gets decreases accordingly. Figure 6.3.shows better performance of Proximity Rule Estimation (PRE) scheme in terms of users than existing open social network filtering (OSN). Proximity Rule Estimation (PRE) achieves 10 to 25% less Memory space of user variation when compared to existing system.

5. CONCLUSION:

In this paper, a secure friend discovery is established based on proximity rules for mobile social networks. The proposed proximity rules estimation (PRE) provided better private security and verifiable proximity computation based on polynomial secure share. Various possible attack messages are prevented from posting on analyzing real traces through proximity rule by getting the feedback forms from the user for friend-like nomenclature and also using relational privacy index. At last, PRE allows users to identify only the acceptable messages that are listed in their social network space, satisfying the user requirements with better filtering technique. Analysis and implementation justifies the feasibility and effectiveness of PRE.

With growing recognition of mobile social networks, it is essential to extend secure and practical protocols to facilitate users to efficiently interrelate with each other. Finally, this paper developed a secure friend discovery protocol for mobile social networks justifying the real use on open social networks with high privacy.

6. SCOPE OF FUTURE WORK

The future work on security is constraint processing and context dependent security constraints and sees if we can apply some of the ideas for Resource Description Framework (RDF) Security. Finally, the role of ontologies is for secure information integration. Standards play an essential role in the expansion of the semantic web.

7. LIMITATION:

Proposed work PSS techniques concentrates only to estimate the proximity rules for filtering in un-preferred messages. Further needs to reduce the strong anomalous attack messages and reduce computation time on estimation of proximity rule.

8. BIBLIOGRAPHY:

[1] Victoria Bobicev, Marina Sokolova, "An Effective and Robust Method for Short Text Classification", 2008, Association for the Advancement of Artificial Intelligence.
[2] Bharath Sriram, David Fuhry, Engin Demir, Hakan Ferhatosmanoglu,Murat Demirbas, "Short Text Classification in Twitter to Improve Information Filtering", SIGIR'10, July 19–23, 2010, Geneva, Switzerland.
[3] Ismail Sengor Altingovde, Engin Demir, Fazli Can, Özgür Ulusoy, "Site-Based Dynamic Pruning for Query Processing in Search Engines", SIGIR'08, July 20–24, 2008, Singapore.
[4] Kerstin Severinson Eklundh and Henrry Rodriguez, "Coherence and Interactivity in Text-Based Group Discussions around Web Documents", Proceedings of the 37th Hawaii International Conference on System. 2004.
[5] Jennifer Golbeck, "Combining Provenance with Trust in Social Networks for Semantic Web Content Filtering" 2003.
[6] Lalana Kagal, Massimo Paolucci, Naveen Srinivasan, Grit Denker, Tim Finin, Katia Sycara, "Authorization and Privacy for Semantic Web Services" 2000
[7] Gordon V. Cormack,José María Gómez Hidalgo, Enrique Puertas Sánz, "Spam Filtering for Short Messages" 2007
[8] Thomas R. Lynam and Gordon V. Cormack, "Online Spam Filter Fusion", SIGIR'06, August 6–11, 2006, Seattle, Washington, USA.
[9] Byoung-Tak Zhang and Young-Woo Seo,"PersonalizedWeb-Document Filtering Using Reinforcement Learning". 2001
[10] 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, FEBRUARY 2013.