Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Privacy Based Image and Comment Sharing on Online Social Networks Based on Short Text Classification

M. Muthubrindha, Dr. A. Valarmathi
Department of Computer Applications, Anna University College (BIT Campus), Trichy, Tamilnadu, India

Abstract: Social networks are today one of the most popular interactive medium to share, communicate, and distribute a significant amount of human life information. Most common interactive medium to communicate is online social network. There are various types of information shared by users such as image, messages, audio, videos and so on.Online social network offer very less amount of security at the time of uploading images. So information filtering approach can be used to filter the information in online social networks.In social media, information filtering is very expensive and difficult to process because of various functions included in these social media. We can provide privacy preserving approach in images based Adaptive privacy policy prediction approach to select users based on social context. The aim of the present work is design framework, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. The most important effort is implement Short Text Classifier (STC) is used to extracting and selecting the tokens from comments. Then using filtered rules and block list approaches to eliminate unwanted messages and also block the friends who are send the unwanted messages continuously and they are automatically filtered by server.

Keywords: Online Social Network, Privacy Policy, Filter Unwanted Messages, Image and Commend

I. INTRODUCTION

Nowadays social network take an important role in our daily life ,social network used to connected the people together by grouping themself .so they can share their information, happiness ,audio,video,image,text, etc.., . Images are take an important part of our life, because images are used to connect the people together in social network. Sharing image and content are increasing such as YouTube, flicker, Google+, etc..,. Most probably youngster are used to shared their personal information of images, through the social network which was hidden from their family members and staff. By sharing this images and content they not had been think about the privacy .the recent study's shows that 90% of images shared through the social network by the youngster. While sharing image privacy is an most important that poplar socialnetwork of face book was introduce tag system in this we have to decided whom we like to share,it only share to that tag persons along, but their friend of friend can view or download or else share to others ,so still privacy logging .to overcome this problem design framework, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. Then exploit machine Learning (ML) approach to implement text mining techniques to automatically assign with each short text message a set of categories based on its substance. The most important effort is implement short text classifier (STC) is used to extracting and selecting the tokens from comments. Then using filtered rules and block list approaches to eliminate unwanted messages and also block the friends who are send the unwanted messages continuously and they are automatically filtered by server.

II. PROBLEM STATEMENT

Privacy is an emerging challenge in OSNs, and a number of researchers have examined different aspects of the privacy problem. Researchers have examined the privacy model of existing OSNs, demonstrating that sites often leak numerous types of privacy information. So implement Policy based personalization is applicable in many different contexts. It adapts a service in specific context according user defined policies. It assigns a category to each image and shows only those images to the user which are of his interest. In this scenario, policy based personalization represent the ability of the user to filter wall messages according to filtering criteria suggested by him. But in privacy based policy system, difficult to filter comments which are posted for image and can't policy for messages. So design the system offers a powerful rule layer utilizing a flexible language to specify Filtering Rules (FRs), by which users can state what substances, should not be showed on their walls. FRs can maintain a variety of different filtering criteria that can be combined and customized according to the user requirements.. Additionally, the system gives the support for user-defined Black Lists (BLs), that is, lists of users that are temporarily prevented to post any kind of messages on a user wall.

III. EXISTING SYSTEM

Social Networking is one of the major technological phenomena of the Web 2.0, with hundreds of millions of people participating. Social networks enable a form of self-expression for users, and help them to socialize and share content

with other users. In spite of the fact that content sharing represents one of the prominent features of existing Social Network sites, Social Networks yet do not support any mechanism for privacy settings for shared content. The sharing of personal data has emerged as a popular activity over online social networking sites like Facebook. As a result, the issue of online social network privacy has received significant attention in both the research literature and the mainstream media. Images are now one of the key enablers of users' connectivity. Sharing takes place both among previously established groups of known people or social circles (e.g., Google+, Flickr or Picasa), and also increasingly with people outside the users social circles, for purposes of social discovery- to help them identify new peers and learn about peers interests and social surroundings. Existing system propose a two-level framework which according to the user's available history on the site, determines the best available privacy policy for the user's images being uploaded.

Description of the System

The A3P system consists of two main components: A3Pcore and A3P-social. The overall data flow is the following. When a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. In most cases, the A3P-core predicts policies for the users directly based on their historical behavior. If one of the following two cases is verified true, A3P-core will invoke A3P-social: (i) The user does not have enough data for the type of the uploaded image to conduct policy prediction; (ii) The A3Pcore detects the recent major changes among the user's community about their privacy practices along with user's increase of social networking activities (addition of new friends, new posts on one's profile etc). In above cases, it would be beneficial to report to the user the latest privacy practice of social communities that have similar background as the user. The A3P-social groups users into social communities with similar social context and privacy preferences, and continuously monitors the social groups. When the A3P-social is invoked, it automatically identifies the social group for the user and sends back the information about the group to the A3P-core for policy prediction. At the end, the predicted policy will be displayed to the user. If the user is fully satisfied by the predicted policy, he or she can just accept it. Otherwise, the user can choose to revise the policy.

A3P Framework

Users can provide privacy preferences about their data disclosure preferences with their socially connected users via privacy policies. The privacy policy is: A privacy policy P of user u consists of the following components:

- Subject (S): A set of users socially connected to u.
- Data (D): A set of data items shared by u.
- Action (A): A set of actions granted by u to S on D.
- Condition (C): A Boolean expression which must besatisfied in order to perform the granted actions.

A3P- Social

The A3P-social employs a multi-criteria inference mechanism that generates representative policies by leveraging key information related to the user's social context and his general attitude toward privacy. As mentioned earlier, A3Psocial will be invoked by the A3P-core in two scenarios. One is when the user is a newbie of a site, and does not have enough images stored for the A3P-core to infer meaningful and customized policies. The other is when the system notices significant changes of privacy trend in the user's social circle, which may be of interest for the user to possibly adjust his/her privacy settings accordingly. In what follows, we first present the types of social context considered by A3P-Social, and then present the policy recommendation process. Modeling Social Context we observe that users with similar background tend to have similar privacy concerns, as seen in previous research studies and also confirmed by our collected data. This observation inspires us to develop a social context modeling algorithm that can capture the common social elements of users and identify communities formed by the users with similar privacy concerns. The identified communities who have a rich set of images can then serve as the base of subsequent policy recommendation. The social context modeling algorithm consists of two major steps. The first step is to identify and formalize potentially important factors that may be informative of one's privacy settings. The second step is to group users based on the identified factors. We now introduce the policy recommendation process based on the social groups obtained from the previous step. Suppose that a user U uploaded a new image and the A3P-core invoked the A3P-social for policy recommendation. The A3P-social will find the social group which is most similar to user U and then choose the representative user in the social group along with his images to be sent to the A3P-Core policy prediction module to generate the recommended policy for user U. Given that the number of users in social network may be huge and that users may join a large number of social groups, it would be very time consuming to compare the new user's social context attributes against the frequent pattern of each social group. In order to speed up the group identification process and ensure reasonable response time, we leverage the inverted file structure to organize the social group information. The inverted file maps keywords (values of social context attribute) occurring in the frequent patterns to the social groups that contain the keywords.

Disadvantages:

- Existing system focus on sharing data that includes images
- Can't deal with tags and posts that are associated with images
- Difficult analyze short text tags.

IV. PROPOSED SYSTEM

Information filtering systems are designed to classify a stream of dynamically generated information dispatched asynchronously by an information producer and present to the user those information that are likely to satisfy his/her requirements. Focusing on the OSN domain, interest in access control and privacy protection is relatively recent. As future as confidentiality is disturbed, current work is essentially focusing on privacy-preserving data mining methods, that is, protecting data associated to the network, i.e., relations/nodes, while performing social network study. Effort more associated to our schemes is those in the field of access control.

In this field, various dissimilar access control models and associated mechanisms have been proposed so far which essentially differ on the expressivity of the access control policy language and on the way access control is enforced (e.g., centralized vs. decentralized). The majority of these models convey access control requirements in terms of relationships that the requestor should have with the resource holder. We use a related idea to classify the users to which a filtering rule applies. For itself, one of the key elements of our scheme is the availability of an explanation for the message contents to be exploited by the filtering mechanism as well as by the language to express filtering rules. In distinguish no one of the access control models previously cited exploit the content of the resources to enforce access control. We consider that this is an essential difference. Furthermore, the concept of blacklists and their administration are not believed by any of these access control models. 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 categorization has acknowledged up to now few attentions in the scientific community. Aim of the short text classifier is to recognize and eradicate the positive sentences and categorize the negative sentences in step by step, not in single step. This classifier will be used in hierarchical strategy. The first level task will be classified with positive and negative labels. The second level act as a negative, it will develop gradual membership. This grade will be used as succeeding phases for filtering process. Short text classifier includes text representation, machine learning based classification.

V. SYSTEM ARCHITECTURE

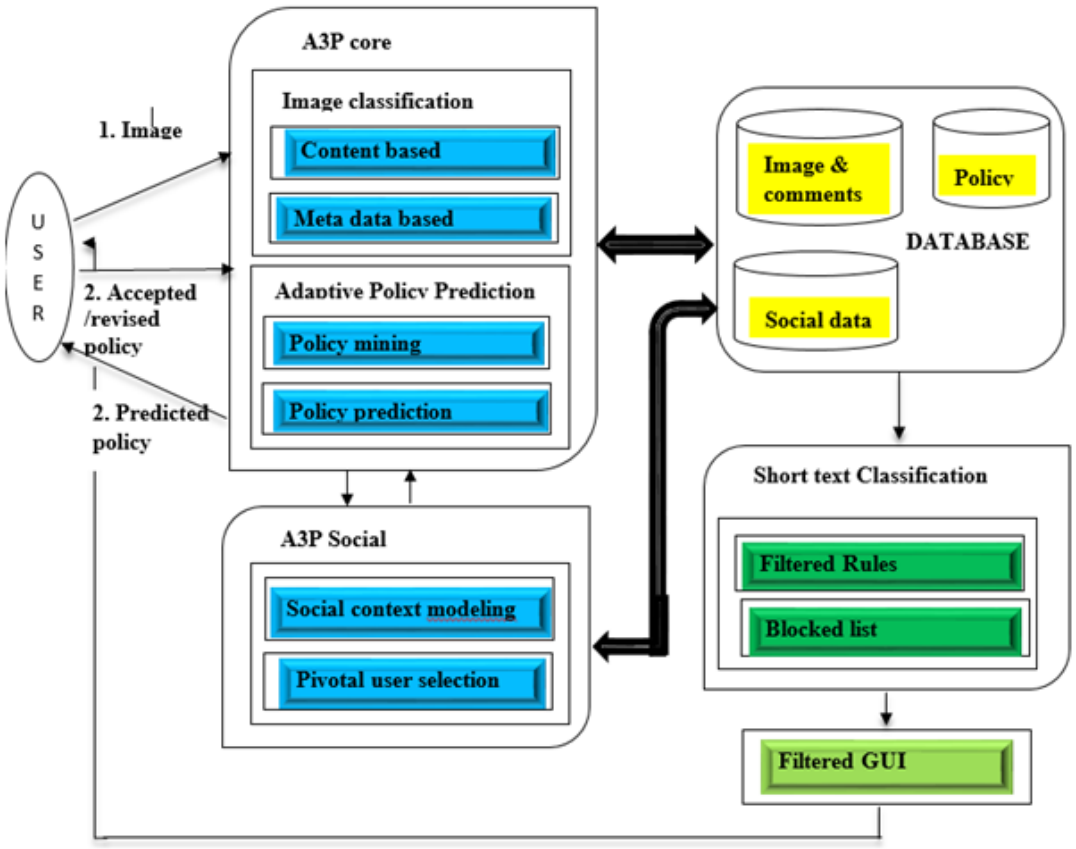

Fig. 1.Architecture

VI. MODULES DESCRIPTION

Social media managers are often found in the marketing and public relations departments of large organizations. In face book, **GUI** is a type of user interface that allows users to interact with users through graphical icons and visual indicators such as secondary notation, as opposed to text-based interfaces, typed command labels or text navigation. GUIs were introduced in reaction to the perceived steep learning curve of command-line interfaces (CLI),which require commands to be typed on the keyboard.Well-designed graphical user interfaces can free the user from learning complex commandlanguages. On the other hand, many users find that they work more effectively with a command-driven interface, especially if they already know the command language.

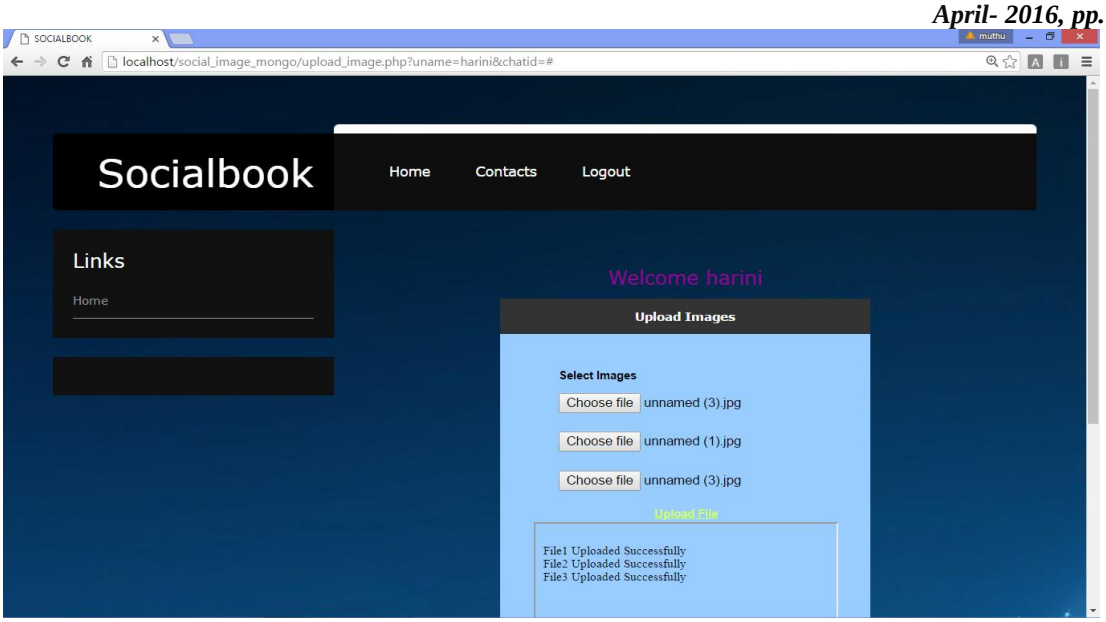

Fig. 2.Upload image of social book

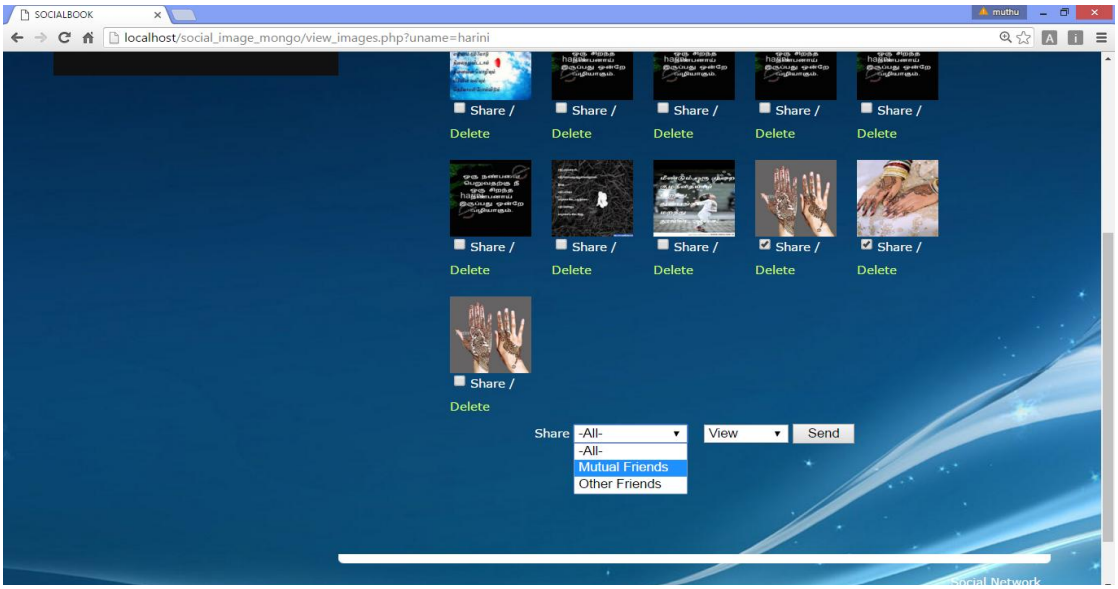

Fig. 3.Upload image of social book selecting categories

Now apply the A3P core framework for sharing the image through the social book.it produce the privacy policy in this user can choose whom that want to share.

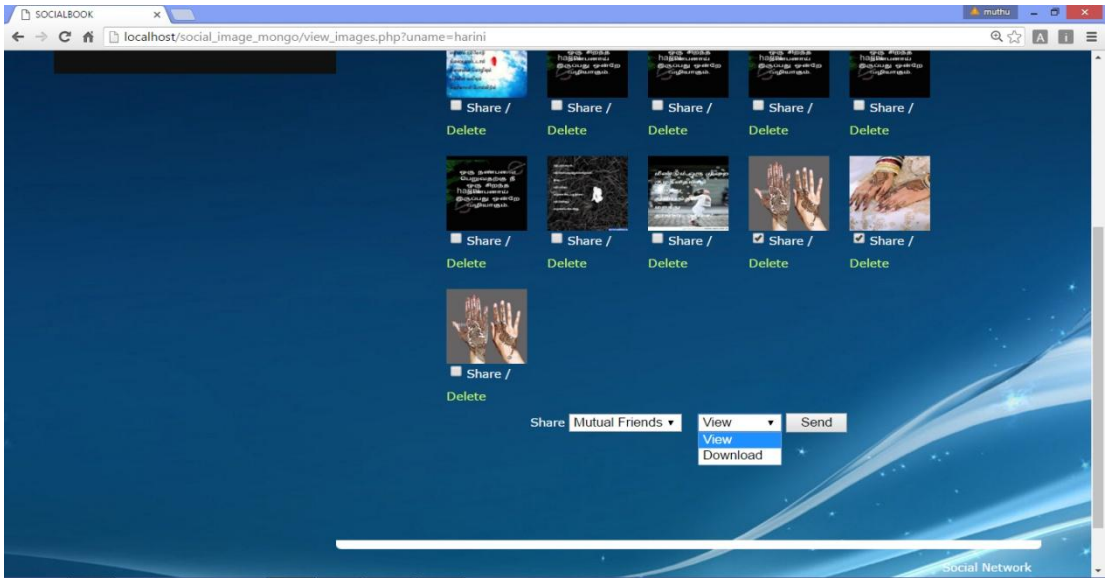

Fig. 4.Sharing image of social book select categories of view or download

Here A3P social framework will apply in this,it deals with whether that particular image must be view or download to their shared people

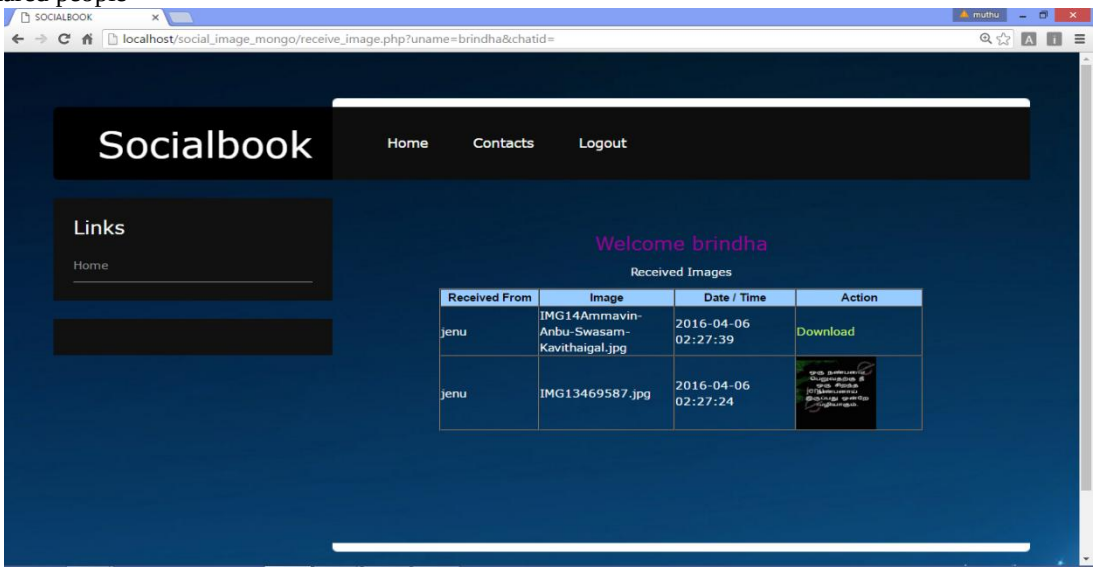

Fig. 5.Receive image of social book

Image has been received by that pariticular user it show that image have the privcy of social book , that means if it have that privacy policy is applied .in that two opptions are avaiable one is downloaded and another one is view.Downloaded opption means people can have the permession to download image.At the same time view opption have the permission to view aloan.

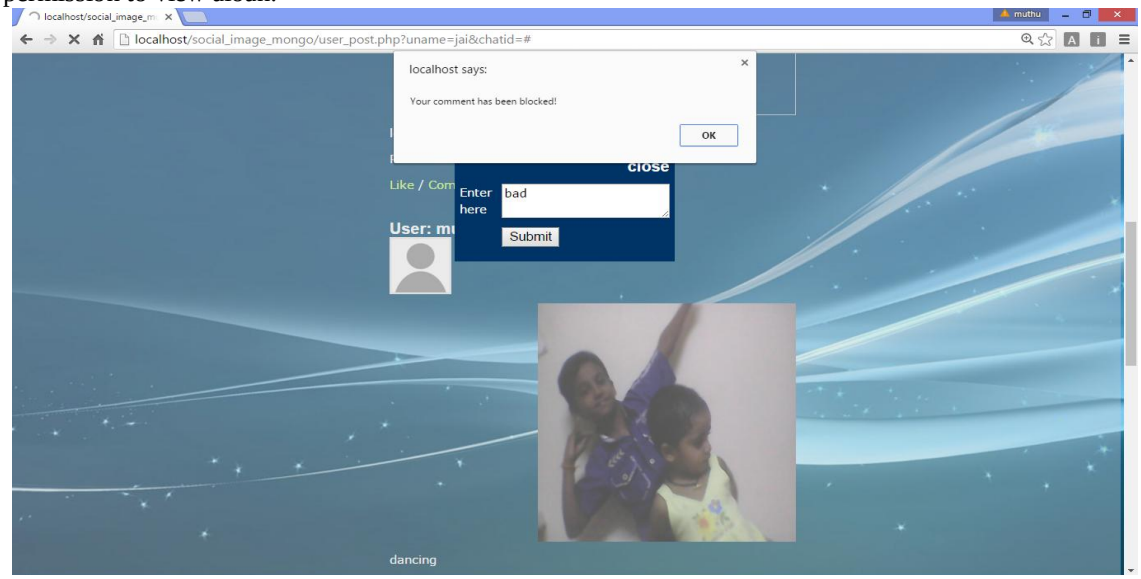

Fig. 6.Unwanteded comments blocked of social image

Commend has been blocked in the since for posting comment for the image, posted by the user that comment was unwanted that is negative word posted to that image means that commends will blocked(hidden to their friends)It done by the short text classification.

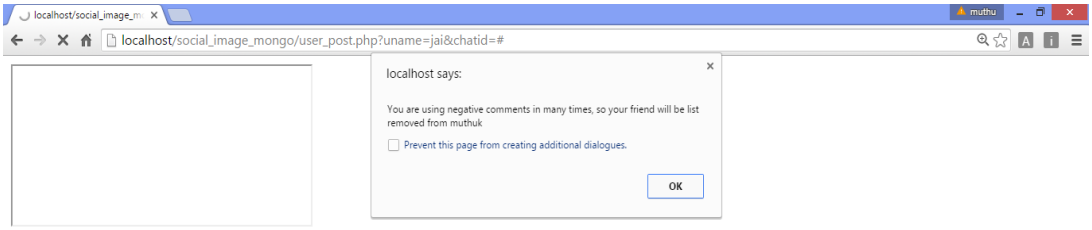

Fig. 7.Friend was removed of social book

If that user send continually unwanted message means that user will remove from the mutual friend list of the posted user

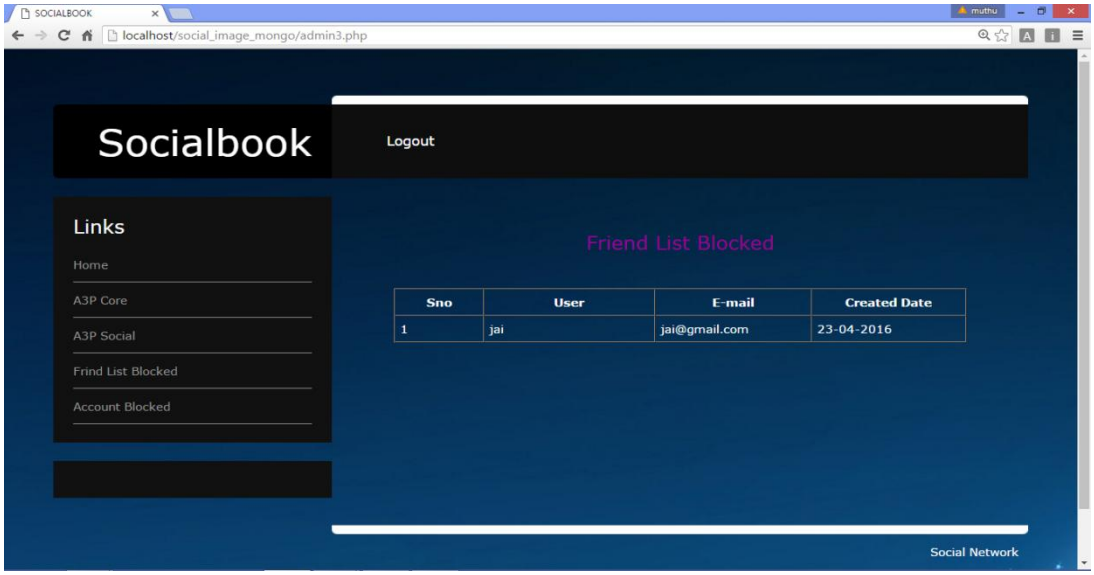

Fig. 8.Friend list blocked details of social image

In this module, we designan automated system, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. The architecture in support of OSN services is a three-tier structure. The first layer commonly aims to provide the basic OSN functionalities (i.e., profile and relationship management). Additionally, some OSNs provide an additional layer allowing the support of external Social Network Applications (SNA)1. Finally, the supported SNA may require an additional layer for their needed graphical user interfaces (GUIs).

VII. CONCLUSION

In this project, we are using the software system to filter unwanted messages from social network walls. We can design filtered GUI for user based on user actions, behaviors and reputation in OSN, which might imply to enhance OSN with audit mechanisms. On extending the Machine Learning (ML) text categorization techniques to automatically assign with each short text message a set of categories based on its content. Then 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.

VIII. FUTURE WORK

As part of future work, to implement cryptographic techniques and various filtering techniques to secure OSN home page. And also extend the work in privacy based uploaded video content sharing sites. And also analyze various language reviews to specify the unwanted comments.

REFERENCES

[1] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.

[2] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, "Social circles: Tackling privacy in social networks," in Proc. Symp. Usable Privacy Security, 2008.

[3] P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer, L. F. Cranor, N. Gupta, and M. Reiter, "Tag, you can see it!: Using tags for access control in photo sharing," in Proc. ACM Annu. Conf. Human Factors Comput. Syst., 2012, pp. 377–386.

[4] A. Mazzia, K. LeFevre, and A. E.,, "The PViz comprehension tool for social network privacy settings," in Proc. Symp. Usable Privacy Security, 2012.

[5] S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, "Privacy-aware image classification and search," in Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inform. Retrieval, 2012, pp. 35–44.

