International Journal of Current Research and Modern Education (IJCRME)
ISSN (Online): 2455 - 5428
(www.rdmodernresearch.com) Volume I, Issue I, 2016

PRIVACY BASED IMAGE AND COMMENT SHARING ON ONLINE SOCIAL NETWORKS BASED ON SHORT TEXT CLASSIFICATION

N. Sangeetha* & R. Selvakumar**

* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Assistant Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:

Social medias 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 networks (OSNs) are one of the most popular interactive medium to communicate, share and dissipate a considerable amount of human life information. The main issue in online social networks is the users have less control over the filtering mechanism of unwanted messages that posted on their walls. This paper presents an overview of various methods used for text classification in online social networks.As the amount of content will be very huge information filtering is used. 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 user wall, various data posted as user policies and shared by multiple friends. 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. And also extend the work to implement information filtering approach to be used to give users the ability to automatically monitor the messages written on their own walls, by filtering out unwanted messages and comments about images. The aim of the present work is 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.

Key Words: Online Information Services, Web-Based Services & Content Sharing Sites

1. Introduction:

Nowadays social network take an important role in our daily life ,social network used to connected the people together by grouping themselves .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 youngsters are used to share 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 social network of face book was introduce tag system in this we have to decide 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.Text classification is one of the major techniques for processing text data. In the new era, the online information is growing rapidly. Text categorization can be defined as the classification of documents into a fixed number of predefined categories. We can classify the text categorization approaches into rule based and machine learning based approaches. For improving the privacy and security of online social networks we can use text classification methods in messages that are posted by the users. Users can communicate and share information in the form of text, image, audio, video data etc. through OSNs. Day by day a huge amount of information is exchanged through OSNs, so it is very important to ensure the filtering mechanisms in OSNs.

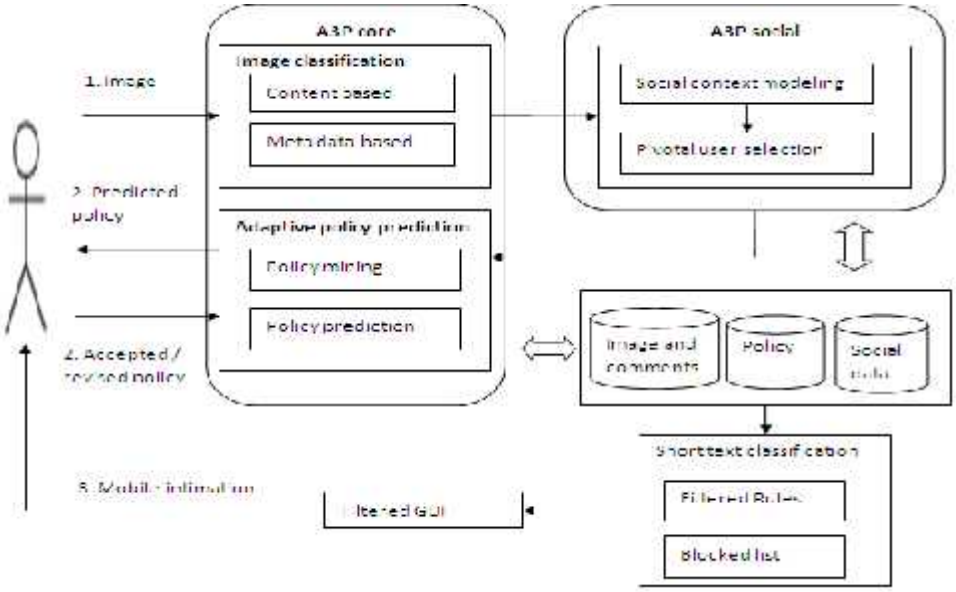

Figure 1: System overview

The Role of Image's Content and Metadata:

In spite of the fact that content sharing represents one of the important features of existing Social Network sites, Social Networks yet do not sustain any mechanism for collaborative execution of privacy settings for shared content [2]. Social networking sites are used by a huge number of users all over the world. It provides different features to the customers like chatting, posting comments, image sharing, video chatting etc. Images are now one of the key enablers of user's 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. However, semantically rich images may reveal content sensitive information [2]. Consider a photo of a student's 2012 graduation ceremony, for example. It could be shared within a Google+ circle or Flickr group, but may unnecessarily expose the students. Sharing images within online content sharing

sites, therefore, may quickly lead to unwanted disclosure and privacy violations [3], [4]. Further, the persistent nature of online media makes it possible for other users to collect rich aggregated information about the owner of the published content and the subjects in the published content [3], [2], [4]. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

2. Literature Review:

"Privacy Suites: Shared Privacy for Social Networks,"

Creating privacy controls for social networks that are both expressive and usable is a major challenge. Lack of user understanding of privacy settings can lead to unwanted disclosure of private information and, in some cases, to material harm. We propose a new paradigm which allows users to easily choose "suites" of privacy settings which have been specified by friends or trusted experts, only modifying them if they wish. Given that most users currently stick with their default, operator-chosen settings, such a system could dramatically increase the privacy protection that most users experience with minimal time investment. This approach has many parallels in other security configuration domains in which delegating security policy to a trusted authority is common. These tasks are similar to the social networking privacy problem in that they are tedious and require frequent updates. For instance, more than 50 million users have installed the Ad Block Plus plugin for Mozilla Firefox, which allows users to select a trusted source to create a blacklist of advertising domains. Automatic patching and anti-virus software have become ubiquitous in modern operating systems, allowing users to select a trusted source for updates as new vulnerabilities are discovered. Privacy Suites could also be created directly through existing configuration UIs, exporting them to the abstract format. Hybrid design interfaces could also be designed, enabling new public interfaces to be built for users to manipulate their settings. The disadvantage of a rich programming language is less understandability for end users. Given a sufficiently high-level language and good coding practice, motivated users should be able to verify a Privacy Suite. The main goal is transparency, which is essential for convincing influential users that it is safe to use.

"Social Circles: Tackling Privacy in Social Networks,"

Face book has recently implemented a feature called Friend Lists, which allows users to more easily set privacy policies for a collection of friends by manually creating a list of friends and setting privacy policies for the list. For example, a user may create friend lists called College, Workplace, and Salsa Club, and present a different view of their personal profile to friends on each of these lists. Unfortunately, while Friend Lists are a step towards a more usable mechanism for controlling privacy in social networking services, it has a major drawback: many users have more friends than they can categorize into lists effectively. To alleviate the burden of categorizing a large number of users into meaningful lists, we propose a technique called Social Circles Finder for generating these lists automatically. We posit that clusters of densely and closely connected friends, or social circles as we call them, can be viewed as uniform groups from the perspective of privacy settings. In other words, we believe that users would present (mostly) consistent profiles with all friends in a social circle, and therefore social circles provide a meaningful categorization of friends for setting privacy policies. As an example, members of a college athletic team are "friends" of one another and hence (personal) information propagates easily among them. Hence, team members would probably want to present the same profile to all other members and thus set the same privacy policy for all of them. Social Circles Finder will be able to identify the

athletic team (possibly with a small chance of incorrect categorization) as a social circle. Social Circles Finder would be able to, with proper integration into the Face book platform, provide the above features not just when users are browsing their friends, but also when they are adding new friends.

"Tag, You Can See It! Using Tags for Access Control in Photo Sharing,"

Systems that use such tags to define access-control policies have been prototyped. However, the usability of tag based access control has not been investigated using users' own content, tags, and access-control policies. In this paper, we employ an 18-participant laboratory study using participants' own photos to explore the feasibility of tag-based access-control rules for photo sharing. Although tag-based access control could potentially apply to broader categories of digital content, we draw on photo sharing as an initial case study both because users have varied access-control preferences for photos and because systems that allow users to tag photos are already in use. We found that organizational tags could be repurposed to create efficient and reasonably accurate access-control rules. When participants tagged photos with access control in mind, they were typically able to develop coherent strategies and create tags that supported significantly more accurate rules than those created from organizational tags alone. We also observed that participants understood the concept of tag based rules and were able to actively engage in rule suggestion. We designed an exploratory laboratory study during which participants performed three separate tagging tasks. The first task focused exclusively on organizational tagging to help a user organize and search her photos, while the second and third tasks focused on organizational tagging in combination with tagging for access control. These tasks provided insight into participants' tagging behaviors and strategies. Tags from these tasks were also used to create machine-generated access-control rules that roughly approximated users' policies.

"The PViz Comprehension Tool for Social Network Privacy Settings,"

The motivation for enabling privacy-oriented search is two-fold: First, users should be able to retrieve resources about themselves (or about their children or other relatives) published by third parties at an early stage, so that measures such as contacting owners of servers or providers can be taken. Second, the degree of privacy of the information need behind a query can be ambiguous for a search engine. In this paper, we use classifier outputs to conduct privacy oriented search, which enables users to directly discover private information about a specific topic. In addition, we perform privacy-based diversification of search results (i.e. retrieving a "mixture" of private and public content) to minimize the risk of user dissatisfaction in cases where queries are ambiguous with respect to the privacy aspect of the information need. The motivation for this is analogous to topic-related diversification: to cover different information needs and provide an overview over the whole search result space rather than just a list of top-ranked results. We are aware that building alarm systems for private content and enabling privacy-oriented search can be seen as contradicting goals; privacy-oriented search is not negative per se, as it can be used for retrieving private content users are comfortable to share, and, more importantly, can help with the early discovery of privacy breaches. However, as with almost every technology, it requires sensible handling and constructive usage. In this paper we applied classification using various visual and textual features to estimate the degree of privacy of images. Classification models were trained on a large-scale dataset with privacy assignments obtained through a social annotation game. We made use of classifier outputs to compute ranked lists of private images as well as search results.

"I Know What You Did Last Summer! Privacy-Aware Image Classification and Search in Proc. 22nd ACM Conf. Hypertext Hypermedia,"

The motivation for enabling privacy-oriented search is two-fold: First, users should be able to retrieve resources about themselves (or about their children or other relatives) published by third parties at an early stage, so that measures such as contacting owners of servers or providers can be taken. Second, the degree of privacy of the information need behind a query can be ambiguous for a search engine. In this paper, we use classifier outputs to conduct privacy oriented search, which enables users to directly discover private information about a specific topic. In addition, privacy-based diversification of search results (i.e. retrieving a "mixture" of private and public content) to minimize the risk of user dissatisfaction in cases where queries are ambiguous with respect to the privacy aspect of the information need is performed. The motivation for this is analogous to topic-related diversification: to cover different information needs and provide an overview over the whole search result space rather than just a list of top-ranked results. Building alarm systems for private content and enabling privacy-oriented search can be seen as contradicting goals is known; privacy-oriented search is not negative per se, as it can be used for retrieving private content users are comfortable to share, and, more importantly, can help with the early discovery of privacy breaches. However, as with almost every technology, it requires sensible handling and constructive usage. In this paper we applied classification using various visual and textual features to estimate the degree of privacy of images. Classification models were trained on a large-scale dataset with privacy assignments obtained through a social annotation game. Classifier outputs to compute ranked lists of private images as well as search results are made.

3. Implementation:

Social Network Creation:

Social network refers to interaction among people in which they create, share, and/or exchange information and ideas in virtual communities and networks. A social network manager is the individual in an organization trusted with monitoring, contributing to, and filtering, measuring and otherwise guiding the social media presence of a brand, product, individual or corporation. The role is similar to that of a community manager on a website forum or public relations representative. 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 command languages. 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.

A3P Core:

A3P core contains two major components such as

- ✓ Image classification
- ✓ Adaptive policy prediction

Each user images are first categorized into content and metadata. Then privacy policies of each images can be categorized and analyzed for predict the policy. So we adopting two stages approach for policy recommendation than applying the common

one-stage data mining approaches to mine both image features and policies together. The two-stage approach allows the system to employ the first stage (i.e., the image classification) to classify the new image and find the candidate sets of images for the subsequent policy recommendation. Moreover, combining both image features and policies into a single classifier would lead to a system which is very dependent to the specific syntax of the policy. If a change in the supported policies were to be introduced, the whole learning model would need to change.

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.

Social Group Updation:

In this module, we design an 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).

Short Text Classification:

The filtering rules should allow users to state constraints on message creators. Thus, creators on which a filtering rule applies should be selected on the basis of several different criteria; one of the most relevant is by imposing conditions on user profile's attributes. In such a way it is, for instance, possible to define rules applying only to young creators, to creators with a given religious/ political view, or to creators that we believe are not expert in a given field (e.g. by posing constraints on the work attribute of user profile). This means filtering rules identifying messages according to constraints on their contents. In order to specify and enforce these constraints, we make use of the text classification.

Evaluation Criteria:

In performance evaluation, we calculate the precision and recall values. The Precision (P), that permits to evaluate the number of false positives, Recall (R), that permits to evaluate the number of false negatives, and the overall metric F-Measure, defined as the harmonic mean between the above two index. Then our method efficient to filter the unwanted messages from the user walls and status of block lists.

4. Result and Discussion:

A total of 506 respondents accessed the survey. One-hundred-eleven (21.9%) were not currently affiliated with the college Institution where we conducted our study, or did not have a email address within that Institution's domain. They were not allowed to take the rest of the survey. A separate set of 32 (8.2%) participants had taken part in a previous pilot survey and were also not allowed to take the survey. Of the remaining respondents, 318 subjects actually completed the initial calibration questions. Out of this set, 278 (87.4%) had heard about FB, 40 had not. In this group, 225 (70.8%) had a profile on FB, 85 (26.7%) never had one, and 8 (2.5%) had an account but deactivated it. Within those three groups, respectively 209, 81, and 7 participants completed the whole survey. We focus our analysis on that set - from which we further removed 3 observations from the non-members group, since we had reasons to believe that the responses had been created by the same individual. This left us with a total of 294 respondents.

5. Conclusion:

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.

6. 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.

7. 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.
6. L. Geng and H. J. Hamilton, "Interestingness measures for data mining: A survey," ACM Comput. Surv., vol. 38, no. 3, p. 9, 2006.
7. Image-net data set. Available: www.image-net.org, Dec. 2013.
8. S. Jones and E. O'Neill, "Contextual dynamics of group-based sharing decisions," in Proc. Conf. Human Factors Comput. Syst., 2011, pp. 1777–1786.

9. A. Kaw and E. Kalu, Numerical Methods with Applications: Abridged, Raleigh, North Carolina, USA: Lulu.com, 2010.
10. K. Lerman, A. Plangprasopchok, and C. Wong, "Personalizing image search results on flickr," CoRR, vol. abs/0704.1676, 2007.
11. A. Singhal, "Modern information retrieval: A brief overview," IEEE Data Eng. Bullet., Speicial Issue on Text Databases, vol. 24, no. 4, pp. 35-43, Dec. 2001.
12. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, "A3p: Adaptive policy prediction for shared images over popular content sharing sites," in Proc. 22nd ACM Conf. Hypertext Hypermedia, 2011, pp.261–270.