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

Ms. N. Bhavani[1], R. Packialakshmi[2], R. Raji[3], S. Suganya[4], S. Swetha[5]
[1, 2, 3, 4, 5] Department of Information Technology
[1, 2, 3, 4, 5] Saranathan college of engineering, Tiruchirapalli-620012,Tamilnadu,India

Abstract- *Social media is one of the most popular interactive medium to communicate and share various types of information 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. Hence privacy preserving approach based on Adaptive privacy policy prediction is provided to select users based on social context. Information filtering approach is implemented in order to give users the ability to automatically monitor the messages written on their own walls, by filtering out unwanted messages and comments. Short text classifier (STC) is used to extract and for selecting the tokens from comments. Filtered rules and block list approaches are used to eliminate unwanted messages and to block friends who send unwanted messages continuously which are automatically filtered by server.*

Keywords- Images, comments, PHP, Wamp server

I. INTRODUCTION

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. However, semantically rich images may reveal content sensitive information. Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations. 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. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information. Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. One of the main reasons provided is that given the amount of shared information ,this process can be tedious and error-prone. Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings .However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed. In this paper, an Adaptive Privacy Policy Prediction (A3P) system is adopted which aims to provide users a hassle free privacy settings experience by automatically generating personalized policies.

II. LITERATURE SURVEY

1. 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. And 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 AdBlock 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.

2. Social Circles: Tackling Privacy in Social Networks

Facebook 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, propose a technique called Social Circles Finder for generating these lists automatically and 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 Facebook platform, provide the above features not just when users are browsing their friends, but also when they are adding new friends.

3. 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, 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, 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 and 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. Participants understood the concept of tag based rules and were able to actively engage in rule suggestion were observed. An exploratory laboratory study during which participants performed three separate tagging tasks are designed. 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 behaviours and strategies. Tags from these tasks were also used to create machine-generated access-control rules that roughly approximated users' policies.

4. The PViz Comprehension Tool for Social Network Privacy Settings

Online social networking systems have existed for many years, but the changing features of these systems, coupled with mass adoption, have exacerbated the problems of privacy and presentation management. Such groupings are not always explicit, and existing policy comprehension tools, such as Facebook's Audience View, which allows the user to view her profile as it appears to each of her friends, are not naturally aligned with this mental model. In this paper, we introduce PViz, an interface and system which corresponds more directly with the way users model groups and privacy policies applied to their networks. PViz allows the user to understand the visibility of her profile according to natural sub-groupings of friends, and at different levels of granularity. An extensive user study comparing PViz to current privacy comprehension tools (Facebook's Audience View and Custom Settings page) is conducted. Despite requiring users to adapt to new ways of exploring their social spaces, our study revealed that PViz was comparable to Audience View for simple tasks, and provided a significant improvement for more complex, group based tasks. In designing PViz, our focus so far has been on the privacy comprehension problem (resolving one's mental model of privacy and visibility with the existing system configuration) and hope to provide improvements in this regard (improved community detection and labeling algorithms). However, that PViz also provides a natural platform for policy control.

5. I Know What You Did Last Summer!:Privacy-Aware Image Classification and Search

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.

III. RELATED WORKS

PHP:

PHP files can contain text, HTML, CSS, JavaScript, and PHP code.PHP code are executed on the server, and the result is returned to the browser as plain HTML. PHP can generate dynamic page content.PHP can create, open, read, write, delete, and close files on the server.PHP can collect form data. It can send and receive cookies. It can add, delete, modify data in your database.PHP can be used to control user-access and can encrypt data. With PHP you are not limited to output HTML. You can output images, PDF files, and even Flash movies. You can also output any text, such as XHTML and XML.

PHP runs on various platforms (Windows, Linux, Unix, Mac OS X, etc.).PHP is compatible with almost all servers used today (Apache, IIS, etc.).It supports a wide range of databases

To start using PHP, you can:

Find..web..host..with..PHP..and..MySQLsupport.Install a web server on your own PC, and then install PHP and MySQL.
Syntax: A PHP script can be placed anywhere in the document. A PHP script starts with <? php and ends with ?>:

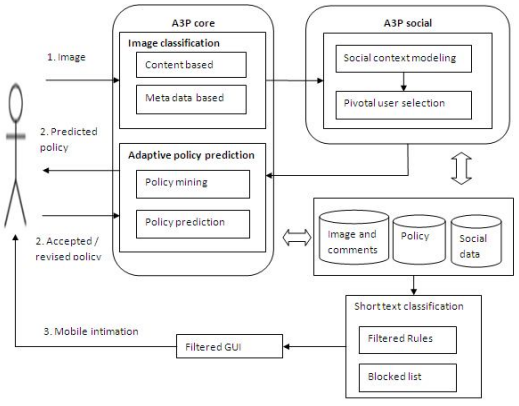
```
<?php
//PHP..code
?>
```

The default file extension for PHP files is ".php".A PHP file normally contains HTML tags, and some PHP scripting code. In PHP, all keywords (e.g. if, else, while, echo, etc.), classes, functions, and user-defined functions are NOT case-sensitive.

MYSQL:

MySQL is the world's most used open source relational database management system(RDBMS) as of 2008 that run as a server providing multi-user access to the number of databases. access to a number of databases. The MYSQL development project has made its source code proprietary agreements. MySQL was owned and sponsored by a single non-profit firm, the Swedish company MySQL AB, now owned by Oracle Corporation.

IV. SYSTEM ARCHITECTURE



Images that is shared on social media are not secured and protected. Hence to provide privacy to the images that we upload, Adaptive privacy policy prediction algorithm is used. This algorithm is classified into two levels A3P core and A3P

social. In A3P core we are extracting the main contents present in the images ie, Metadata. There are two major components in A3P-core: (i) Image classification and (ii) Adaptive policy prediction. For each user, his/her images are first classified based on content and metadata. Then, privacy policies of each category of images are analyzed for the policy prediction.

The A3P-social employs a multi-criteria inference mechanism. This generates representative policies by leveraging key information related to the user's social context and its 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 new to 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. In Social group updation, sorting the keywords (except the social connection) in the frequent patterns in an alphabetical order takes place. Each keyword is associated with a link list which stores social group ID and pointers to the detailed information of the social group. Finally we apply Short text classification algorithm. 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.

V. CONCLUSION & FUTURE WORK

By using STC, comments are tokenized. It eliminates all vowels and remaining words are compared with words already trained in database. If positive words are present, it gets posted on our homepage and spread to others, or else gets blocked and will not reach others homepage. When Offline, we are intimated through SMS if negative comments get posted . We can set allow or block for those comments. If negative comments keep on get posted by a particular member, we can set threshold, and if negative comments exceed that threshold being set ,then that member is blocked from friends with our permission.

REFERENCES

[1] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in Proc.6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006,pp. 36–58.

[2] R. Agrawal and R. Srikant,"Fast algorithms for mining association rules in large databases," in Proc. 20th Int. Conf. Very Large Databases, 1994, pp. 487–499.

[3] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing," in Proc. Conf. Human Factors Comput.Syst., 2007, pp. 357–366.

[4] M. Ames and M. Naaman, "Why we tag: Motivations for annotation in mobile and online media," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 971–980.

[5] A. Besmer and H. Lipford, "Tagged photos: Concerns, perceptions, and protections," in Proc. 27th Int. Conf. Extended Abstracts Human Factors Comput. Syst., 2009, pp. 4585–4590.

[6] D. G. Altman and J. M. Bland ,"Multiple significance tests: The bonferroni method," Brit. Med. J., vol. 310, no. 6973, 1995.

[7] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy