ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

An Improved Privacy Policy Inference over the Socially Shared Images in Social Web Sites

K.Archana[1], Dr. H. Lilly Beaulah[2]

M.E Student, Dept.of Computer Science and Engineering, Mahendra College of Engineering, India[1]

Head of Department, Dept.of Computer Science and Engineering, Mahendra College of Engineering, India[2]

ABSTRACT: 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. With the increasing volume of images users share through social sites, maintaining privacy has become a major problem. Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations. Most content sharing websites allow users to enter their privacy preferences. Unfortunately, in existing system, users struggle to set up and maintain such privacy settings. Existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images. We propose an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. We examine the role of social context, image content, and metadata as possible indicators of users' privacy preferences. We 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. Our solution relies on an image classification framework for image categories which may be associated with similar policies, and a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features**.**

KEYWORDS: A3P core, adaptive privacy policy prediction, hierarchical classification, content-based classification, policy mining.

I. INTRODUCTION

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.

The A3P system consists of two main components: A3P-core 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 A3Psocial: (i) The user does not have enough data for the type of the uploaded image to conduct policy prediction; (ii) The A3P-core 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

DOI: 10.15680/IJIRCCE.2015. 0311127

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. The actual policy will be stored in the policy repository of the system for the policy prediction of future uploads. Bonneau. Proposed the concept of privacy suites which recommend to users a suite of privacy settings that “expert” users or other trusted friends have already set, so that normal users can either directly choose a setting or only need to do minor modification. Similarly, Danezis proposed a machine-learning based approach to automatically extract privacy settings from the social context within which the data is produced. Parallel to the work of Danezis, Adu-Oppong develop privacy settings based on a concept of “Social Circles” which consist of clusters of friends formed by partitioning users’ friend lists. Ravichandran studied how to predict a user’s privacy preferences for location-based data (i.e., share her location or not) based on location and time of day. Fang et al. proposed a privacy wizard to help users grant privileges to their friends. The wizard asks users to first assign privacy labels to selected friends, and then uses this as input to construct a classifier which classifies friends based on their profiles and automatically assign privacy labels to the unlabeled friends. More recently, Klemperer et al. studied whether the keywords and captions with which users tag their photos can be used to help users more intuitively create and maintain access-control policies. Their findings are in line with our approach: tags created or organizational purposes can be repurposed to help create reasonably accurate access-control rules. The aforementioned approaches focus on deriving policy settings for only traits, so they mainly consider social context such as one’s friend list. While interesting, they may not be sufficient to address challenges brought by image files for which privacy may vary substantially not just because of social context but also due to the actual image content. As far as images, authors in have presented an expressive language for images uploaded in social sites. This work is complementary to ours as we do not deal with policy expressiveness, but rely on common forms policy specification for our predictive algorithm.

II. RELATED WORK

In [1] authors mentioned that, Users of online social networking communities are disclosing large amounts of personal information, putting themselves at a variety of risks. Our ongoing research investigates mechanisms for socially appropriate privacy Management in online social networking communities. As a first step, we are examining the role of interface usability in current privacy settings. In this paper we report on our first iterative prototype, where presenting an audience oriented view of profile information significantly improved the understanding of privacy settings.[2]In this paper, we provide a systematic experimental evaluation of several collaborative filtering algorithms to recommend groups for Flickr users. In particular, we design and compare seven Flickr group recommendation models: three memory-based models and four model-based models. Our results suggest that model-based approaches are beneficial compared with memory-based approaches in terms of top-k recommendation metric. Models with tags perform well for sparse data, whereas models without tags are more suitable for dense data. Furthermore, incorporating tags in the recommendation algorithms leads to an Improvement of precision on the top 2% performance.In this work, we intend to produce automatic recommendations of a user’s images to suitable photo-sharing groups. To this end, we begin with analysing user annotations and modeling the shared images in a group. Both visual content and annotation context are then integrated to understand the events or topics depicted in those images [3].Our results demonstrate the need for mechanisms that provide awareness of the privacy impact of users’ daily interactions. Profile FeaturesFacebook profiles can be extensive, including a variety of self reported information (disclosures) as well as details of the user’s social environment, including pictures, friends lists, and messages with friends[5].

III. PROPOSED SYSTEM

We Propose an Adaptive Privacy Policy Prediction (A3P) system which aims to provide users a hassle free privacy settings experience by automatically generating personalized policies. A policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users’ social features. Anna Cinzia Squicciarini developed an Adaptive Privacy Policy Prediction (A3P)system, a free privacy settings system by automatically generating personalized policies. The A3P system handles user uploaded images based on the person’s personal characteristics and images content and metadata. The A3P system consists of two components: A3P Core and A3P

Social. 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. The A3P system handles user uploaded images, and factors in the following criteria that influence one's privacy settings of images:

A) THE IMPACT OF SOCIAL ENVIRONMENT AND PERSONAL CHARACTERISTICS**:**

Social context of users, such as their profile information and relationships with others may provide useful information regarding users' privacy preferences.

For example, users interested in photography may like to share their photos with other amateur photographers.

Users who have several family members among their social contacts may share with them pictures related to family events.

In light of these considerations, it is important to find the balancing point between the impact of social environment and users' individual characteristics in order to predict the policies that match each individual's needs.

Moreover, individuals may change their overall attitude toward privacy as time passes. In order to develop a personalized policy recommendation system, such changes on privacy opinions should be carefully considered.

B) THE ROLE OF IMAGE'S CONTENT AND METADATA:

In general, similar images often incur similar privacy preferences, especially when people appear in the images. For example, one may upload several photos of his kids and specify that only his family members are allowed to see these photos.

Finally propose a new authentication scheme "Color Scheme Authentication".

Instead of just words we propose a system in which authentication is done using colors and numbers. Users can give values from 1 to 8 for the given 8 colors. Users can even give same value for two different colors. This makes the authentication method risk free of shoulder attack, dictionary attack, eves dropping etc.

C) ADVANTAGES OF PROPOSED SYSTEM:

- Automatically generate a policy for each newly uploaded image, also according to users' social features.
- It provide users a hassle free privacy settings experience
- Effectively tackled the issue of cold-start, leveraging social context information.
- Prediction accuracy will be increased, as the system adapts to users' privacy preferences

IV. SIMULATION AND RESULT

1. A3P-Core

Our first experiment compares A3P-core with alternative prediction approaches. In particular, we use a straw man solution as the baseline approach, whereby we sample at random a small set of image settings from the same user and use them to determine a baseline setting (by counting the most frequent items). The baseline settings are applied to all images of the users. Further, we compare the A3Pcore with two variants of itself, in order to evaluate the contribution of each component in the A3P-core made for privacy prediction. The first variant uses only content-based image classification followed by our policy mining algorithm, denoted as "Content Mining". The second variant uses only tag classification followed by the policy mining, denoted as "Tag Mining". All the algorithms were tested against the collected real user policies. Fig. 4 shows the percentage of predicted policies in four groups:

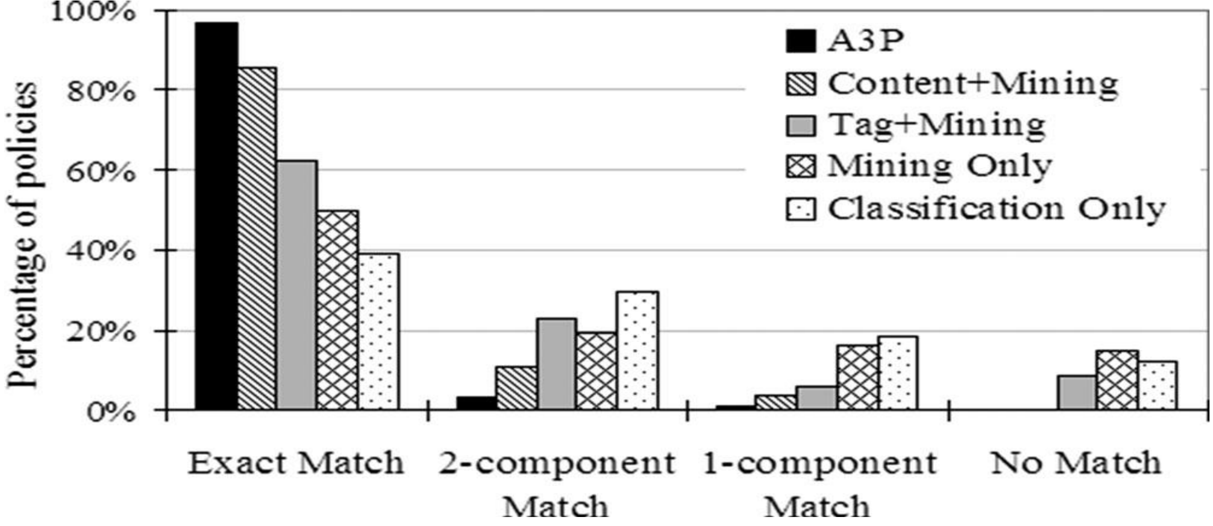
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A3B comparative performance



“Exact Match” means a predicted policy is exactly the same as the real policy of the same image; “x-component Match” means a predicted policy and its corresponding real policy have x components (i.e., subject, action, condition) fully matched; “No match” simply means that the predicted policy is wrong for all components. As shown in the figure, each component of the A3P-core singularly contributes toward policy prediction, however, none of them individually equalizes the accuracy achieved by the A3P-core in its entirety. Specifically, A3P-core has 90 percent exact match and 0 no match. Moreover, pairwise comparisons were made between A3P-core, “Content Mining, “Tag Mining” and the baseline algorithm, corrected using a Bonferroni method.

2. Analysis of Users’ Characteristics

We are also interested in examining whether our algorithm performs better for users with certain characteristics. Therefore, we study possible factors relevant to the performance of our algorithm. We used a least squares multiple regression analysis, regressing performance of the A3P-core to the following possible predictors. Frequency of social network use was measured on a frequency rating scale (1 ¼ daily; 2 ¼ weekly; 3 ¼ monthly; 4 ¼ rarely; 5 ¼ never) with the item ‘How often do you access Social Network Sites?’ _ Privacy settings take time was measured on a Likert Scale (5-point rating scale, where 1 ¼ strongly agree and 5 ¼ strongly disagree) with the item ‘Changing privacy settings for images uploaded on a social site can be very time consuming.’

Result of Direct User Evaluation

Item Type	Count	Ratio
Total Polices	1025	92.1%
Exactly Matched Policies	944	
Policies with 1 error	67	6.4%
Policies with 2 errors	10	1.1%
Policies with 3 errors	4	0.4%

Frequency of sharing pictures was measured using three items (a ¼ 0:69) rated on a Likert scale. Frequency of changing privacy settings was measured using four items (a ¼ 0:86) rated on a Likert scale. An example item is ‘I have changed privacy settings for individual pictures.’ Content of concern was measured using three items (a ¼ 0:81) rated on a Likert scale. An example item is ‘The content of an image is of concern when determining the privacy level for an image.’ Privacy concern was measured using four items (a ¼ 0:76) rated on a Likert scale. An example item is ‘I have had concerns about my privacy due to shared images on social network sites.’

V. CONCLUSION AND FUTURE WORK

We have proposed an Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. We also effectively tackled the issue of cold-start, leveraging social context information. Our experimental study proves that our A3P is a practical tool that offers significant improvements over current approaches to privacy. We also propose a system in which authentication is done using colors and numbers. Users can give values from 1 to 8 for the given 8 colors. Users can even give same value for two different colors. This makes the authentication method risk free of shoulder attack, dictionary attack, eves dropping etc.

REFERENCES

[1]. H. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view," in Proc. Conf. Usability, Psychol., Security, 2008.

[2]. N. Zheng, Q. Li, S. Liao, and L. Zhang, "Which photo groups should I choose? A comparative study of recommendation algorithms in flickr," J. Inform. Sci., vol. 36, pp. 733–750, Dec. 2010.

[3]. J. Yu, D. Joshi, and J. Luo, "Connecting people in photo-sharing sites by photo content and user annotations," in Proc. IEEE Int.Conf. Multimedia Expo, 2009, pp.1464–1467.

[4]. C.-H. Yeh, Y.-C. Ho, B. A. Barsky, and M. Ouhyoung, "Personalized photograph ranking and selection system," in Proc.Int. Conf. Multimedia, 2010, pp. 211–220. [Online]. Available: http://doi.acm.org/10.1145/1873951.1873963.

[5]. K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," in Proc. Brit. Comput Soc. Conf. Human-Comput. Interact. 2008, pp.111–119.

[6]. R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable Privacy Security, 2009.

[7]. J. Bonneau, J. Anderson, and G. Danezis, "Prying data out of a social network," in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining.,2009, pp.249–254.

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

[9]. M. Rabbath, P. Sandhaus, and S. Boll, "Analysing Facebook features to support event detection for photo-based facebook applications," in Proc. 2nd ACM Int. Conf. Multimedia Retrieval, 2012, pp. 11:1–11:8.

[10]. Dan Lin, Sundareswaran.S, Wede.J,"Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites" in Proc. IEEE Int. Volume.27, Issue.1Jan. 1 2015

BIOGRAPHY

K.Archana is a M.E (CSE) Student in the Department of Computer Science and Engineering, Mahendra College of Engineering, Salem, Tamil Nadu, India. She received Bachelor's degree in Information Technology in 2013 from Sona College of Technology, Salem, Tamil Nadu, India. Her research interests' area is Data mining.