International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Survey on A3P System for Image Uploading

Sucheta Shinde[1], Swarupa Kamble[2]

[1]Department of Computer Engineering, RMD Sinhgad School of Engineering, Pune, Maharashtra, India

[2]Assistant Professor, Dept. of Computer Engineering, RMD Sinhgad School of Engineering, Pune, Maharashtra, India

Abstract: ***With the sharing of images on social media such as Facebook, twitter, etc. increases, maintain their privacy becomes the major problem. As user shares their private images on social sites, people expect more tools to allow them to regain control over their privacy. By considering this need, we propose an Adaptive Privacy Policy Prediction (A3P) system which provides user convenient privacy settings by automatically generating personalized policies. To define users' privacy preferences we consider the different factors such as social environment, personal characteristics, image content and metadata. For the images being uploaded, we define the best available privacy policy for the user based on the users' available history on the site. For that we propose a two level framework. A3P system relies on the image classification framework for image categories which may be associated with similar policies and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features.***

Keywords: Social media, content sharing sites, metadata, policy mining, policy prediction

1. Introduction

Social media is a two way communication. It means to communicate, share and interact with an individual or with a large audience. Social networking sites are the most famous sites on the internet and millions of people use them to connect with other people. On these social websites most shared content is images. User of this website uploads their images on the websites and also shares these images with other people. The sharing of images is based on the group of people he/she knows, social circle or public and private environment. Sometimes images may contain the sensitive information. For example, consider a photo of family function. It could be shared with a Google+ circle or Flicker group, but may unnecessarily expose to the college friends. Thus, the sharing of images online sites lead to a privacy violation. The persistent nature of online media, can results in a misuse of one's personal information and its social environment.

Most content sharing sites allow users to enter their privacy preferences like private or public. But recent study shows that user struggles to setup and maintain such privacy settings. Therefore, we need a policy recommendation system which can guide user to easily and properly configure privacy settings. As the amount of information carried within images and their relationship with the online environment causes the existing privacy setting inadequate to address the unique privacy needs of images.

In this paper, we propose an Adaptive Privacy Policy Prediction (A3P) system which provides user convenient privacy settings by automatically generating personalized policies. The A3P system handles user uploaded images and factors in the following criteria that influence ones privacy settings of images:

The impact of social environment and personal characteristics: users' social environment such as their profile information and relationship with other users provide useful information regarding the users' privacy preferences. Also, for the same type of images users have a different opinion. So it is important to find the balancing point between these two to predict the policies that match each individuals needs.

The role of images content and metadata: In general, similar images often incur similar privacy preferences, especially when people appear in the images. Analyzing the visual content may not be sufficient to capture users' privacy preferences. Tags and other metadata are indicative of the social context of the image, including where it was taken and why and also provide a synthetic description of images, complementing the information obtained from visual content analysis.

2. Overview

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 A3P-social: (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 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.

3. Existing Methodology

Bonneau et al. [1] 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 [2] 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 et al. [3] develop privacy settings based on a concept of "Social Circles" which consist of clusters of friends formed by partitioning users' friend lists. Ravichandran et al. [4] 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. [5] 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. [6] 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 for 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 [7] 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.

4. System Architecture

The A3P system is composed of two main building blocks: A3P core and A3P social. The A3P-core focuses on analyzing each individual user's own images and metadata. There are two major components in A3P-core: (i) Image classification and (ii) Adaptive policy prediction. In image classification images are classified based on their contents and then refine each category into subcategories based on their metadata. In content based image classification we consider spatial information of images such as image color, size, shape, texture, symmetry, etc. In metadata based classification we first extract keywords from the metadata associated with an image. Then we derive a representative hypernym from each metadata vector. And at the end we find a subcategory that image belongs to.

The policy prediction algorithm provides a predicted policy of a newly uploaded image to the user for his/her reference. The prediction process consists of three main phases: (i) policy normalization; (ii) policy mining; and (iii) policy prediction. Policy mining uses a hierarchical approach which is carried out in three steps.

In first step we look for popular actions defined by user. In second step we look for the popular actions in the policy containing popular subjects. And in third step we look for popular conditions in the policy containing both popular subjects and conditions. In the policy prediction we uses the strictness level to define hoe strict the policy is? It is generated by major level and coverage rate. Major level is determined by the combination of subject and action in the policy. Coverage rate is determined by the system using conditional components. The A3P-Social offers a community perspective of privacy setting recommendations for a user's potential privacy improvement. It 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.

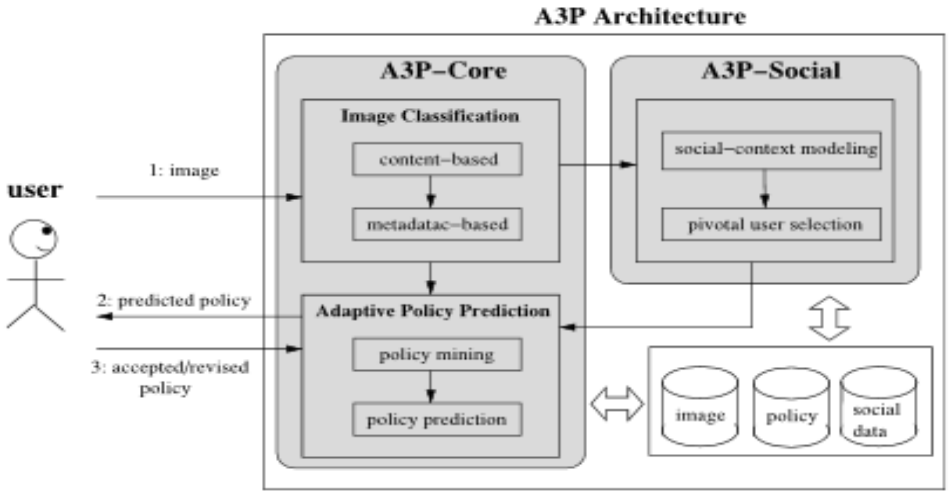

Figure 1: A3P Framework

5. Conclusion

We have proposed an Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacy policy settings for their uploaded images. It provides a framework to deduce the privacy preferences based on the information available for given user. It automatically generates the policy for each newly uploaded image, according to users' social environment. It can increase the efficiency of policy prediction about 90 percent.

References

[1] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.
[2] 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.
[3] 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.
[4] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable Privacy Security, 2009.
[5] A. Mazzia, K. LeFevre, and A. E.,, "The PViz comprehension tool for social network privacy settings," in Proc. Symp. Usable Privacy Security, 2012.
[6] 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.
[7] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data," in Proc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp. 9–14.

Author Profile

Sucheta Shinde received B.E. degree in Computer Science and Engineering in 2011 from Annasaheb Dange College of Engineering and Technology, Ashta (Shivaji University) and pursuing M.E. from RMDSSOE, Warje, Pune.

Swarupa Kamble is working with RMDSSOE, Warje, Pune as an Assistant Professor. She has experience of 5 yrs in the field of teaching and research and her research interests are Image Processing and Data Mining.