Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.206 – 209

Policy Based User-Uploading and Sharing Images on Social Networking Sites Using A3P

Shweta Dinesh Bijwe
Student of Master of Engineering in (CS & IT), HVPM's College of Engineering and Technology, Amravati, India
Shweb350@gmail.com

Prof. P. L. Ramteke
Associate Professor and HOD in Department of (IT), HVPM's College of Engineering and Technology, Amravati, India
pl_ramteke@rediffmail.com

Abstract- Usage of social media's has been considerably increasing in today's world which enables the user to share their personal information like images with other users. This improved technology leads to privacy violation where the users can share large number of images across the network. To provide security for the information, we put forward this paper consisting Adaptive Privacy Policy Prediction (A3P) framework to help users create security measures for their images. The role of images and its metadata are examined as a measure of user's privacy preferences. The Framework determines the best privacy policy for the uploaded images. It includes an Image classification framework for association of images with similar policies and a policy prediction technique to automatically generate a privacy policy for user-uploaded images.

Keywords - social media, content sharing sites, privacy, meta data, a3p

1. Introduction

Images are shared extensively now a days on social sharing sites. Sharing takes place between friends and acquaintances on a daily basis. Sharing images may lead to exposure of personal information and privacy violation. This aggregated information can be misused by malicious users.

To prevent such kind of unwanted disclosure of personal images, flexible privacy settings are required. In recent years, such privacy settings are made available but setting up and maintaining these measures is a tedious and error prone process. Therefore, recommendation system is required which provide user with a flexible assistance for configuring privacy settings in much easier way.

In this paper, we are implementing an Adaptive Privacy Policy Prediction(A3P) system which will provide users a hassle free privacy settings experience by automatically generating personalized policies. The A3P system handles user uploaded images, and factors in the following criteria that influence one's privacy settings of images.

2. LITERATURE SURVEY

Some previous systems shows different studies on automatically assign the privacy settings.One such system which Bonneau et al.[4] proposed shows the concept of privacy suites. The privacy 'suites' recommends the user's privacy setting with the help of expert users. The expert users are trusted friends who already set the settings for the users.

Similarly, Danesiz [3] proposed an automatic privacy extraction system with a machine learning approach from the data produced from the images. Based on the concept of "social circles" i.e forming clusters of friends was proposed by Adu-Oppong et al. [2]Prediction of the users privacy preferences for location-based data (i.e., share the location or no) was studied by Ravichandran et. Al[6]. This was done on the basis of time of the day and location. The study of whether the keywords and captions used for tagging the users photos can be used more efficiently to create and maintain access control policies was done by Klemperer et al.

3. SYSTEM ARCHITECTURE

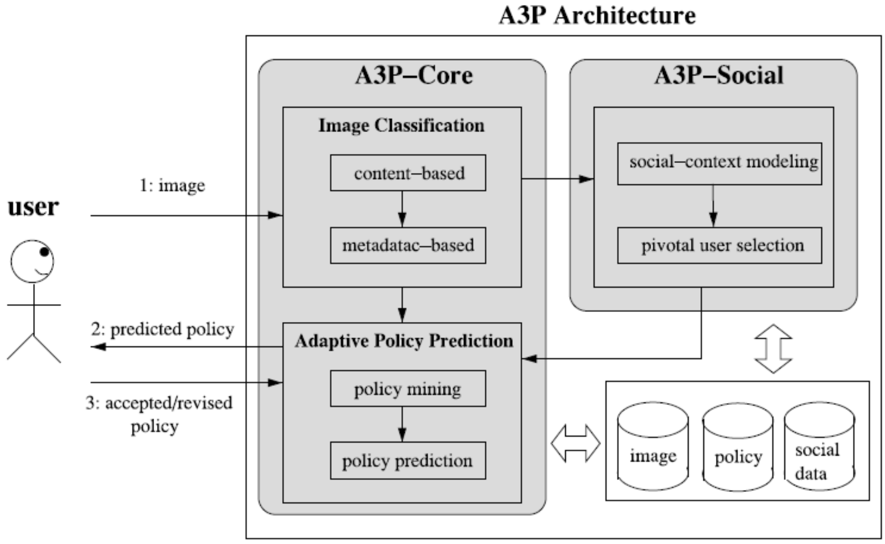

Fig.1 System Overview

A3P stands for Adaptive Privacy Policy Prediction system which helps users to derive the privacy settings for their images The A3P Architecture consists of followings blocks:

- Metadata based Image classification.
- Adaptive policy prediction.
- Look-Up Privacy Policies
- Database

Corresponding to the aforementioned two criteria, the proposed A3P system is comprised of two main building blocks (as shown in Figure 1): A3P-Social and A3P-Core. The A3P-core focuses on analyzing each individual user's own images and metadata, while the A3P-Social offers a community perspective of privacy setting recommendations for a user's potential privacy improvement. We design the interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice.

To assess the practical value of our approach, we built a system prototype and performed an extensive experimental evaluation. We collected and tested over 5,500 real policies generated by more than 160 users. Our experimental results demonstrate both efficiency and high prediction accuracy of our system.

In this work, we present an overhauled version of A3P, which includes an extended policy prediction algorithm in A3P-core (that is now parameterized based on user groups and also factors in possible outliers), and a new A3P-social module that develops the notion of social context to refine and extend the prediction power of our system. We also conduct additional experiments with a new dataset collecting over 1,400 images and corresponding policies, and we extend our analysis of the empirical results to unveil more insights of our system's performance. The rest of the paper is organized as follows. Section2 reviews related works. Section 3 introduces preliminary notions. Section 4 introduces the A3P-core and Section 5 Introduces the A3P-Social. Section 6 reports the experimental evaluation. Finally, Section 7 concludes the paper.

3.1. A3P Core

The A3P Core consist of two major blocks of the framework.

- Content- based Image Classification
- Adaptive Policy Prediction

Adopting a two-stage approach is more suitable for policy recommendation than applying the common one-stage data mining approaches to mine both image features and policies together. Recall that when a user uploads a new image, the user is waiting for a recommended policy. 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. As for the one-stage mining approach, it would not be able to locate the right class of the new image because its classification criteria needs both image features and policies whereas the policies of the new image are not available yet. 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.

3.3.1. Content-Based Image Classification

Specifically, our classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. For each image, the wavelet transform encodes frequency and spatial information related to image color, size, invariant transform, shape,texture, symmetry, etc. Then, a small number of coefficients are selected to form the signature of the image. The content similarity among images is then determined by the distance among their image signatures. The average accuracy of our classifier is above 94%.

Having verified the accuracy of the classifier, we now discuss how it is used in the context of the A3P core. When a user uploads an image, it is handled as an input query image. The signature of the newly uploaded image is compared with the signatures of images in the current image database. To determine the class of the uploaded image, we find its first 'm' closest matches. The class of the uploaded image is then calculated as the class to which majority of the 'm' images belong. If no predominant class is found, a new class is created for the image. Later on, if the predicted policy for this new image turns out correct, the image will be inserted into the corresponding image category in our image database, to help refine future policy prediction. In our current prototype, 'm' is set to 25 which is obtained using a small training dataset.

3.3.2. Adaptive Policy Prediction

The policy prediction algorithm provides a predicted policy of a newly uploaded image to the user for his/her reference. More importantly, the predicted policy will reflect the possible changes of a user's privacy concerns. The prediction process consists of three main phases:

- Policy normalization
- Policy mining
- Policy prediction

Policy normalization: The policy normalization is a simple decomposition process to convert a user policy into a set of atomic rules in which the data (D) component is a single-element set.

Policy mining: Policy mining is carried out within the same category of the new image because images in the same category are more likely under the similar level of privacy protection. The basic idea of the hierarchical mining is to follow a natural order in which a user defines a policy.

Steps of policy mining

Step 1: This process apply association rule mining on the subject components of the policies of the new image. With the association rule mining we select the best rules according to one of the interestingness measure i.e., support and confidence which gives the most popular subjects in policies.

Step 2: This process apply association rule mining on the action components. Similar to the first step we will select the best rules which will give most popular combinations of action in policies.

Step 3: This process mine the condition component in each policy set. The best rules are selected which gives us a set of attributes which often appear in policies.

Policy Prediction: The policy mining phase may give us many policies but our system needs to show the best one to the user. Thus, this approach is used to choose the best policy for the user by obtaining the strictness level. The Strictness level decides how "strict" a policy is by returning an integer value. This value should be minimum to attain high strictness. The strictness can be discovered by two metrics: a major level and coverage rate. The major level is determined with the help of combinations of subject and action in a policy and coverage rate is determined using the condition statement. Different integer values are assigned according to the strictness to the combinations and if the data has multiple combinations we will select the lowest one. Coverage rate provides a fine-grained strictness level which adjusts the obtained major level. For example a user has to 5 friends and two of them are females. Hence if he specifies policy as “friends”=male, then the coverage rate can be calculated as (3/5)=0.6. Hence, the image is less restricted if the coverage rate value is high.

4. CONCLUSION

In this paper we examine the role of social context, image content, and metadata as possible indicators of users’ privacy preferences with the increasing volume of images users share through social sites, maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need, we propose an adaptive privacy policy prediction (a3p) system to help users compose privacy settings for their images..a3p system in used, which provide users easy and properly configured privacy setting for their uploaded image. By using this we can easily prevent unwanted discloser and privacy violations. Unwanted discloser may lead to misuse of one’s personal information .users automate the privacy policy settings for their uploaded images with the help of adaptive privacy policy prediction (a3p). Based on the information available for a given user the a3p system provides a comprehensive framework to infer privacy preferences. A3p system is a practical tool.

References

[1] Smitha Sundareswaran and Joshua Wede, ”Privacy Policy Inference of User-Uploaded Images on Content Sharing sites*”.IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING*,VOL. 27,NO. 1, JANUARY 2015

[2] 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

[3] 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.

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

[5] 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.

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