An Efficient Technique to Control Images on Content Sharing Sites

Tejasvini S. Baviskar,Neha L. Jain,Gauri A. Bhosale,Sneha M. Chaudhari & Prof. U. R. Patole (M.Tech)
SVIT COE, Chincholi, Nashik.

Abstract - *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. We examine the role of social context, image content, and metadata as possible indicators of users privacy preferences. Images are now one of the key enablers of users connectivity. Social Network is an emerging E-service for content sharing sites (CSS). It is emerging service which provides a reliable communication, through this communication a new attack ground for data hackers; they can easily misuses the data through these media. Some users over CSS affects users privacy on their personal contents, where some users keep on sending unwanted comments and messages by taking advantage of the users' inherent trust in their relationship network.*

Key Words: **Online information services, web-based services, Adaptive Privacy Policy Prediction (A3P), A3P-Core, A3P- Social, Polar Fourier Transform (PFT)**

1.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 discovery-to help them identify new peers and learn about peers interests and social surroundings. However, semantically rich images may reveal content sensitive information. 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 BApos family members and other friends.

1.1 Problem Statement

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. Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly congure privacy settings. 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. The A3P system handles user uploaded images that inuence ones privacy settings of images.

2. LITERATURE SURVEY

Using privacy programming a privacy suite can be created by an expert. Privacy Suites could also be created directly through existing configuration UIs or exporting them to the abstract format. Privacy-Aware Image Classification and Search is a technique to automatically detect private images, and to enable privacy-oriented image

A tag based access control of data isis a system that creates access-control policies from photo management tags. Every photo is incorporated with an access grid for mapping the photo with the participant's friends.

Adaptive Privacy Policy Prediction (A3P) system is Personalized policies can be automatically generated by this system. It makes use of the uploaded images by users and a hierarchical image classification is done. Images content and metadata is handled by the A3P system .

2.1 Existing System

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.

2.2 Proposed Scheme

The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. In proposed System an Adaptive Privacy

Policy Prediction (A3P) system that helps users automate the privacy policy settings for their uploaded images.
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.

3. SYSTEM OVERVIEW

- The impact of social environment and personal characteristics:

Users may have drastically different opinions even on the same type of images. For example, a privacy adverse person may be willing to share all his personal images while a more conservative person may just want to share personal images with his family members. 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.

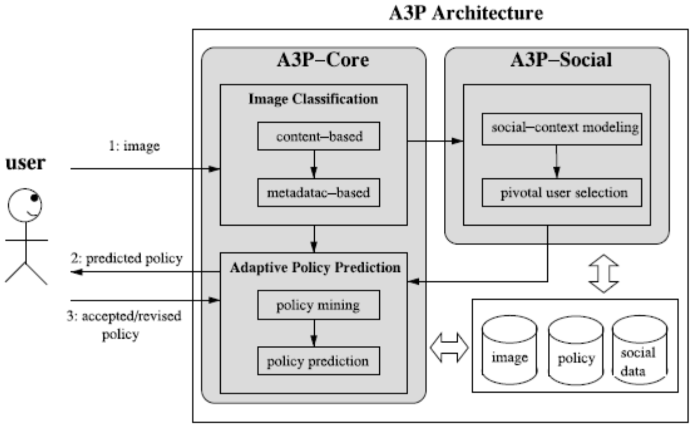

Fig.1 System ovrview

- 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.

3.1 Implementation

- **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.

- **A3P Core**

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. 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 to classify the new image and find the candidate sets of images for the subsequent policy recommendation.

Advantages:
Maintain both efficiency and high prediction accuracy of a system.
1) A3P-CORE
2) A3P-SOCIAL

4. MATHEMATICAL MODEL

INPUT: Input Image

PROCESSING:
Select input image
Load user de_ned association rule for restrictions.
Select one or more rule from the list.
Apply all rules to selected users.
Save all setting related to the image and selected user(s).

OUTPUT: Restriction on user to view/access contents on the speci_ed image.

FUNCTIONS: createPolicy(), generateUserPolicies(), uploadImage(), apply-PolicyOnImage(), publishImage(), setComments(), viewPost()....

Let S be the System s=[I,O,P,F]
Where,
F = f1,f2,f3.....set of functions

f1() is a function used to create policies
f2() is a function and used to generate user de_ned policies
f3() is a function and used to upload an image
f4() is a function and used to apply policy to all selected user(s)
....
fN() is a function and used to access/view the image only for _ltered user(s)
O= Set of output application
Where,
O = Can access/view only _ltered user(s)
P = p1, p2, p3,... set of policies
I = I1, I2, I3.....
SUCCESS:
Filtered user can access / view the speci_ed image if it has any association
rule.

FAILURE:
Any user can access / view the speci_ed image if it has not any association
rule.

5. USE CASE DIAGRAM

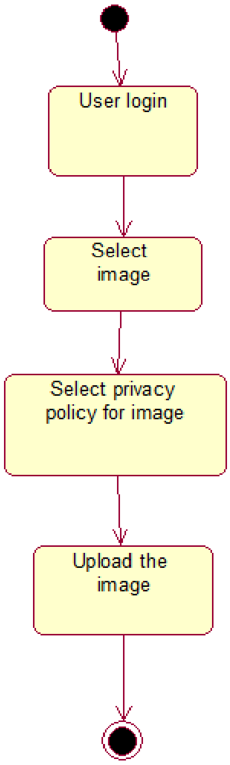

Fig 2.Activity Diagram

6. CONCLUSIONS

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. It is an emerging service which provides a reliable communication, through this a new attack ground from an un-authored person can easily misuses the data through these media.

ACKNOWLEDGEMENT

This research work was support by Prof. U. R. Patole, SVIT COE Nashik. We thank him for guiding us and providing insight which greatly assisted our research work. We also thank Prof. S. M. Rokade, H.O.D. SVIT COE Nashik for his constant motivation. We would also like to show our gratitude to Dr. Prof. S. A. Patil, Principal SVIT COE Nashik and thank him to their constant encouragement and support.

REFERENCES

[1] H.-M. Chen, M.-H. Chang, P.-C. Chang, M.-C. Tien, W. H. Hsu,
and J.-L. Wu, “Sheepdog: Group and tag recommendation for flickr photos by automatic search-based learning,” in Proc. 16th
ACM Int. Conf. Multimedia, 2008, pp. 737–740.
[2] M. D. Choudhury, H. Sundaram, Y.-R. Lin, A. John, and D. D.
Seligmann, “Connecting content to community in social media
via image content, user tags and user communication,” in Proc.
IEEE Int. Conf. Multimedia Expo, 2009, pp.1238–1241.
[3] L. Church, J. Anderson, J. Bonneau, and F. Stajano, “Privacy stories:
Confidence on privacy behaviors through end user programming,”
in Proc. 5th Symp. Usable Privacy Security.
[4] R. da Silva Torres and A. Falc~ao, “Content-based image retrieval:
Theory and applications,” Revista de Inform_atica Te_orica e Aplicada,
vol. 2, no. 13, pp. 161–185,.
[5] R. Datta, D. Joshi, J. Li, and J. Wang, “Image retrieval: Ideas, influences,
and trends of the new age,” ACM Comput. Surv., vol. 40, no. 2, p. 5,.
[6] J. Deng, A. C. Berg, K. Li, and L. Fei-Fei, “What does classifying
more than 10,000 image categories tell us?” in Proc. 11th Eur. Conf.
Comput. Vis.: Part V, 2010, pp. 71–84. [Online]. Available: http://
portal.acm.org/citation.cfm?id=1888150.1888157
[7] 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.

[8] L. Geng and H. J. Hamilton, "Interestingness measures for data
mining: A survey," ACM Comput. Surv., vol. 38, no. 3, p. 9,.

[9] Image-net data set. [Online]. Available: www.image-net.org,

[19] A. Kaw and E. Kalu, Numerical Methods with Applications:
Abridged., Raleigh, North Carolina, USA: Lulu.com.