Adaptive Privacy Policy Prediction (A3P) System for Privacy Setting of User-Uploaded Images

Ms. Shevanta N. Kalshetti
Dept of Computer Science
[1]NBN Sinhgad College Of Engineering,Solapur,GATE NO.38/1/B,OFF.Solapur University, Kegaon,Solapur-413255,Maharashtra,India.

Abstract- *Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for the images, which are shared through social sites as maintaining privacy has become a major problem. We address Adaptive Privacy Policy Prediction (A3P) to help users to compose privacy setting for their images to help users control access to their shared content..Use the two level framework for identifying the role of image content, social context & metadata for privacy preferences. We determine the best available privacy policy for the user's images being uploaded which gives the policy prediction algorithm to automatically generate a policy for each newly uploaded image.*

Keywords- Adaptive Privacy Policy Prediction (A3P), A3P-Core, A3P-Social, Privacy setting configuration for Images, Privacy analysis of images

I. INTRODUCTION

An A3P system that helps users automates the privacy policy settings for their uploaded images. Provide a two-level framework which according to the user's available history on the site which determines the best available privacy policy for the user's images being uploaded.

We also effectively tackled the issue of cold start, leveraging social context information.

As Today, for every single piece of content shared on sites like Face book ,the up loader must decide which of his friends, group members, and other Facebook users should be able to access the content. As a result, the issue of privacy on sites like Face book has received significant attention in both the research community and the mainstream media. Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations.
Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure 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 proposed A3P system is comprised of two main building blocks: A3P-Core and A3PSocial.

A3P-core: (I) Image classification and (ii) Adaptive policy prediction.

User images are first classified based on content and metadata. Privacy policies of each category of images are analyzed for the policy prediction. Content-based classification algorithm compares image signatures defined based an efficient and yet accurate image similarity approach. Classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. The metadata-based classification groups images into subcategories under classified baseline categories. A3P social will be invoked by the A3P-core.

1.1 PURPOSE

OBJECTIVES:

1. Design an Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacy policy settings for their uploaded images.
2. Provide a two-level framework which determines the best available privacy policy for the user's images being uploaded.
3. Effectively tackled the issue of cold-start, leveraging social context information.

SCOPE:

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.

II. LITERATURE REVIEW

Following are some existing studies and approaches for Adaptive Privacy Policy Prediction System for Privacy Setting Of User-Uploaded Images on Content Sites.

Bonneau et al. [7] 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.

Danezis [8] 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. [15] 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. [30] 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. [28] 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.

Klemperer et al. [20] 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 inline 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. 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.

Since need to create a system which can assist users to easily and properly configure privacy settings for maintaining privacy for the increasing volume of images users sharing through social sites and within online content sharing sites which leads to unwanted disclosure and privacy violations.

System aims to provide users a hassle free privacy settings experience by automatically generating personalized policies for the user's images being uploaded.

III. MATERIALS AND METHODS

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, and factors in the following criteria that influence one's privacy settings of images:

1. The impact of social environment and personal characteristics.
2. The role of image's content and metadata.

Corresponding to the aforementioned two criteria, the proposed A3P system is comprised of two main building blocks as shown in Fig. 1: A3P-Social and A3P-Core.

A. A.A3P Core – The A3P-core focuses on analyzing each individual user's own Images and metadata.

B. B.A3P Social-A3P-Social offers a community perspective of privacy setting recommendations for a user's potential privacy improvement.

3.1 Image Classification

To obtain groups of images that may be associated with similar privacy preferences, we propose a hierarchical image classification which classifies images first based on their contents and then refine each category into subcategories based on their metadata. Images that do not have metadata will be grouped only by content.

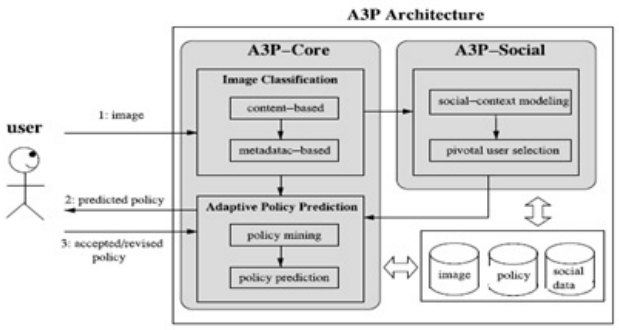

Figure 1 . A system overview showing the A3P Architecture for generating predicted policy for the user uploaded images.

1. Content-Based Classification - Based on an efficient and yet accurate image similarity approach.
2. Metadata-Based Classification- The metadata-based classification groups images into subcategories under classified baseline categories.

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 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.

3.3.1 Adaptive Policy Prediction-

The prediction process consists of three main phases: (I) policy normalization; (II) policy mining; and (III) policy prediction.

I Policy mining-

Propose a hierarchical mining approach for policy mining. The basic idea of the hierarchical mining for given image, a user usually first decides who can access the image, then what specific access rights (e.g., view only or download) should be given.

II Policy Prediction

The policy mining phase may generate several candidate policies while the goal of our A3P system is to return the most promising one to the user. Thus, use the 'strictness level' approach to choose the best candidate policy that follows the user's privacy The policy mining phase may generate several candidate policies while the goal of our A3P system is to return the most promising one to the user. Thus, use the 'strictness level' approach to choose the best candidate policy that follows the user's privacy tendency. The strictness level is a quantitative metric that describes how "strict" a policy is.

III A3P Social

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.

IV. RESULTS

Result of A3P system is a predicate policy for the user uploaded image obtained by three separate questions for every images: (i) who can view the image? (ii) Who can comment? and (iii) who can add notes, tags, and download it?. For each question, the user may choose one among the following options: only you, family only, friends only, social network contacts, and everyone. Our system architecture and policy mining algorithm can easily adapt to different formats of policies.

As in the system architecture first component A3P core made privacy prediction uses two variants content based image classification followed by policy mining algorithm denoted as "Content+Mining". The second variant uses only tag classification followed by the policy mining, denoted as "Tag+Mining". Graph shows the percentage of predicted policies in four groups: "Exact Match", "x-component Match", "No match". Specifically, A3P-core has 90 percent exact match and 0 no match.

Results are reported in Table below. As a final result A3P system can accurately predict preferences will lead to an acceptable level of privacy setting for user's uploaded images.

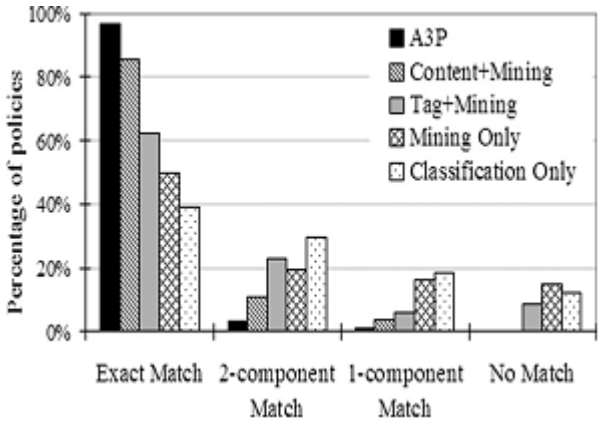

Figure: 2. A percentage of generated predicted policy by the A3P Core.

TABLE 1 Table captions should be placed above the table

Method	View	Comment	Tag, Notes, Download	Overall
A3P Core	92.48%	92.48%	92.63%	92.53%
Propagation	66.12%	66.82%	68.64%	66.84%
Tag Only	87.54%	87.03%	86.64%	87.01%

V. CONCLUSION

Advantages:

1. This system helps users automate the privacy policy settings for their uploaded images.
2. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user uploaded image.
3. Also effectively tackled the issue of cold-start, leveraging social context information.

Future Scope:

In future we can extend this module for social networking sites for user Uploaded Images and extend the security mechanisms for every images being uploaded on social sites.

VI. ACKNOWLEDGEMENT

I feel profound happiness in forwarding this dissertation report as an image of sincere efforts. The successful dissertation reflects my work effort of my guide in giving me good information.

My sincere thanks to respected Prof. B. R. Solunke, my Guide and ME Coordinator who has been a constant source of inspiration and guiding star in achieving my goal & for giving valuable guidelines for completing this dissertation. I give my special thanks to respected Prof. A. A. Phatak, H.O.D.(CSE), for giving me his valuable support and cooperation to enable me to complete my dissertation successfully.

I express my deep sense of gratitude to Dr. S. D. Nawale our Principal for his constant interest and encouragement throughout the completion of my dissertation.

Goal makes us to do work. Vision is more important than goal which makes us to do work in the best way to make work equally the best. I thanks to all CSE department staff members for their support and guidance.

I am also thankful to my parents and friends for their extended support and valuable guidance.

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] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.

[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] 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.

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

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

[7] 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.

[8] H.-M. Chen, M.-H. Chang, P.-C. Chang, M.-C. Tien, W. H. Hsu,and J.-L. Wu, "Sheepdog: Group and tag recommendation forflickr photos by automatic search-based learning," in Proc. 16thACM Int. Conf. Multimedia, 2008, pp. 737–740.

[9] 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.

[10] 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.

[11] 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.

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