Authentication Privacy Policy Preserving Of User Uploaded Images on Social Media

[1]BBTS MRUNALINI, [2]C Venkatesh, [3]G. Sneha
[1,2,3]KG Reddy College Of Engineering And Technology,

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. 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. 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 on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features.

KEY POINTS: - privacy policies, authentication, A3P, Social network, policy prediction

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+, Flicker 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 []. Consider a photo of a student's 2012 graduation ceremony, for example. It could be shared within a Google+ circle or Flicker group, but may unnecessarily expose the student sBApos family members and other friends. Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations [3]. Further, the persistent nature of online media makes it possible for other users to collect rich aggregated information about the owner of the published content and the subjects in the published content [3]. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information. 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 [1], [11], [12], [14]. 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 [7].

2. LITERATURE SURVEY

However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images [3], [5], [9], due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed. In this paper, 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, and factors in the following criteria that influence one's privacy settings of images: 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. However, using common policies across all users or across users with similar traits may be too simplistic and not satisfy individual preferences. Users may have drastically different opinions even on the same type of images.

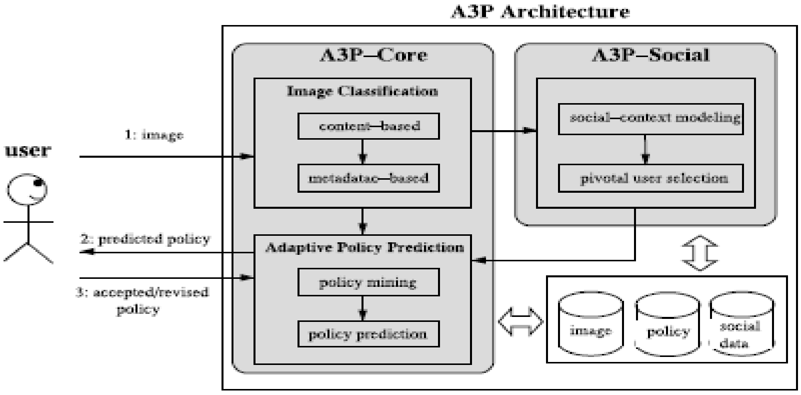


Fig. 1. System overview.

3. THE PROPOSED SYSTEM

A3P POLICY:

Proposed A3P system is comprised of two main building blocks (as shown in Fig. 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. A preliminary discussion of the A3P-core was presented in [10]. 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 data set 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. Section 2 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.

OBJECTIVES

- To gain new understanding of cryptographic models and techniques, in order to face current and future security challenges.
- To consolidate and strengthen the scientific excellence of cryptography using honey cipher
- It is not possible to hacking, it is multi way translation to convert the security
- Cryptography security system is to protect information resources at less cost than the value of the information that is being protected.
- Determining acceptable costs involves weighing the cost of the security versus the benefits of the security.
- It is translate single form of text into multiple structures.
- If the hacker hacking this he cannot find the Original honey form.
- There are multiple structures are generated from the single honey structures.
- Equation is converting the honey structure characters into hexadecimal characters.
- These hexadecimal characters are associated with ASCCII character symbols.
- These ASCII Character Symbols are received by the receiver as a cipher teat

METHODOLOGY

We create a policy named A3P where this can be activated with two different filds A3P core and A3P social. Mainly this policy is used for security purpose and it is used to activate the content or metadata while uploading an image in social content sites.usually we have only privacy settings which we go online and access them but the difference occurs at online and offline policy.this policy is activated through offline.so that our access can't be recorded by online sites.

4. IMPLEMENTATION

4.1 System Admin

The system admin is responsible for providing authorization for specified users and can do some operations such as view uploaded images, view the searching history, view all image ranking and view all users, search images and logout. We hand-classified the tags into six categories, selected subjectively by identifying major themes in the set of all tags: Person, Location, Place, Object, Event, and Activity. Then we associated photos with a each category, according to the tags attached to the photo, and observed privacy differences between photos in the different categories. Note that since each photo may have multiple tags from different categories associated with it, a photo may be counted in multiple categories. To simplify the task of hand-classification, we only classified frequently recurring tags: the top-fifth most frequently used tags for each of the 81 users, resulting in 1538 distinct tags. The tags were classified according to their text, without examining any images; for example, the tags `Mom' or `Marc' was both categorized as Person. Three members of our team classified about 500 tag each, with the option to flag a tag as "difficult to categorize". The "difficult" tags were discussed as a group; if a consensus could not be reached, the tag was left as uncategorized, leaving 1295 categorized tags. The ratio of public photos to non-public photos for each tag category can be seen in Figure 2. For example, of photos that had Person tags, 72% were marked as private. For each category, the number of 5

Corresponding public and private photos is also shown in the figure (for instance, there were 3063 public photos with a Person tag). The belovefigure findings have actionable implications that identify both choices for system designers, and topics for future research. There are opportunities to support and influence users' privacy decision-making process by changing available settings and providing information, simulations, and recommendations. Specifically, we identify five directions suggested by our work.

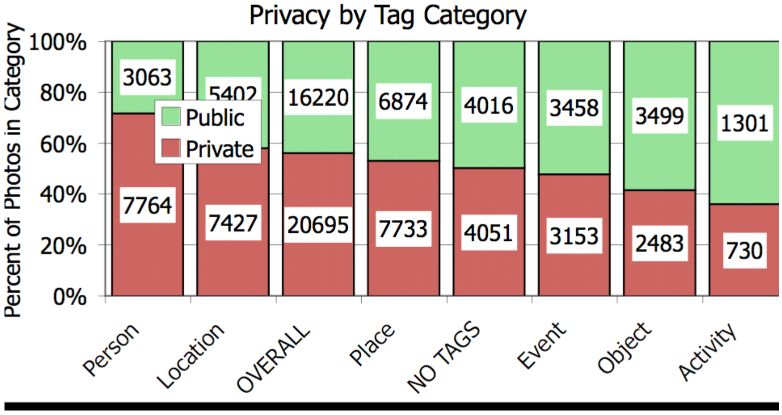


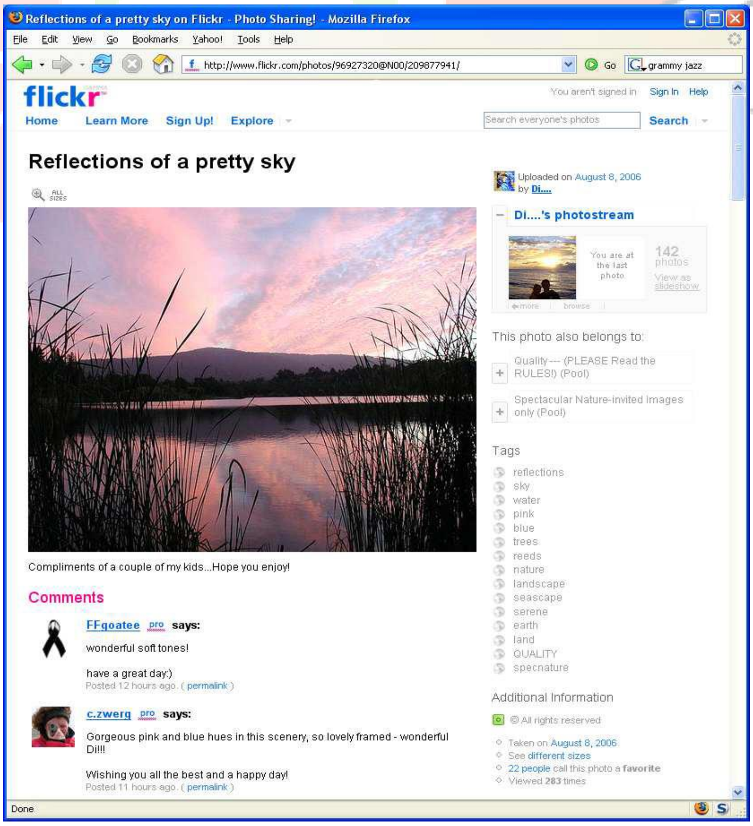
Fig 2: privacy by tag category

4.2 Upload Images

In this module, the user can upload n number of images by their policies If user want to upload new image then he has enter some fields like image name, image color, image description, image type, image usage, browse the image file and upload. After uploading successfully he will get a response from the server. Initially new uploaded image rank is zero. After viewing that image rank will re-rank. The photo sharing site Flicker is one of the earliest and more popular examples of the new generation of Web sites, labeled social media, whose content is primarily user-driven. Other examples of social media include: blogs (personal online journals that allow users to share thoughts and receive feedback on them), Wikipedia (a collectively written and edited online encyclopedia), and Del.icio.us and Dig (Web sites that allow users to share, discuss, and rank Web pages, and news stories respectively). The rise of social media underscores a transformation of the Web as fundamental as its birth. Rather than simply searching for, and passively consuming, information, users are collaboratively creating, evaluating, and distributing information. In the near future, new information-processing applications enabled by social media will include tools for personalized information discovery, applications that exploit the "wisdom of crowds" (e.g., emergent semantics and collaborative.

Social media sites share four characteristics:

(1) Users create or contribute content in a variety of media types;
(2) Users annotate content with tags;
(3) Users evaluate content, either actively by voting or passively by using content;
(4) Users create social networks by designating other users with similar interests as contacts or friends. In the process of using these sites, users are adding rich metadata in the form of social networks, annotations and ratings.



http://www.flickr.com/photos/96927320@N00/209877941/

Reflections of a pretty sky

Uploaded on August 8, 2006 by Di....

Di....'s photostream

You are at the last photo

142 photos

View as slideshow

Compliments of a couple of my kids...Hope you enjoy!

Comments

FFgoatee pro says:

wonderful soft tones!

have a great day:)
Posted 12 hours ago. (permalink)

c.zwerg pro says:

Gorgeous pink and blue hues in this scenery, so lovely framed - wonderful Di!!!

Wishing you all the best and a happy day!
Posted 11 hours ago. (permalink)

This photo also belongs to:

- Quality --- (PLEASE Read the RULES!) (Pool)
- Spectacular Nature-invited Images only (Pool)

Tags

- reflections
- sky
- water
- pink
- blue
- trees
- reeds
- nature
- landscape
- seascape
- serene
- earth
- land
- QUALITY
- specnature

Additional Information

© All rights reserved

- Taken on August 8, 2006
- See different sizes
- 22 people call this photo a **favorite**
- Viewed **283** times

Fig.3: Anatomy of Flicker

4.3 End User

In this module, there are n numbers of users are present. User should register before doing some operations. And register user details are stored in user module. After registration successful he has to login by using authorized user name and password. Login successful he will do some operations like view my details, search images, request secrete key and logout. The user click on my details link then the server will give response to the user with all details such as user name, phone no, address, e mail ID and location. Before searching any images user should request a authorization to admin, then the admin will provide an authorization for particular user and send to the user. After getting an authorization user can search the images base on query or keyword and field like image name, image color, and image usage and image type. And server will give response to the user, then that image rank will be increased.

5. CONCLUSION

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.

6. ACKNOLEDGEMENT

I authored this paper on Authentication Privacy Policy Preserving Of User Uploaded Images on Social Media, with the support of our guide, RAMBABU M, Assoc.Professor, in KG Reddy College of Engineering & Technology,Hyderabad. We are thankful to our chairman, K..Krishna Reddy garu for his support. Finally I am indebted to my family members for providing a peaceful environment.

REFERENCES

[1]A. Acquits 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] R. Agrawal and R. Srikant,“Fast algorithms for mining association rules in large databases,” inProc. 20th Int. Conf. Very Large Data Bases, 1994, pp. 487–499.

[3].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.

[4] 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.

[5] 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.

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

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

[8] 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.

[9]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 flicker photos by automatic search-based learning,” in Proc. 16th ACM Int. Conf. Multimedia, 2008, pp. 737–740.

[10] 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.