ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Efficient Approach in Preserving Image Privacy on Social Sites

Chinthakunta Neelima
M.Tech Student,
Vignana Bharathi Institute of Technology.

Rajasekhar Jelli
Assistant Professor,
Vignana Bharathi Institute of Technology.

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.

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.

LITERATURE SURVEY

Some previous systems shows different studies on automatically assign the privacy settings. One such system which Bonneau et al.[2] 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 [4] 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. [3]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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

EXISTING SYSTEM:

- 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.
- 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.

DISADVANTAGES OF EXISTING SYSTEM:

- Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations.
- 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.
- The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

PROPOSED SYSTEM:

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.
- 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.

ADVANTAGES OF PROPOSED SYSTEM:

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.

SYSTEM ARCHITECTURE

A3P FRAMEWORK

Privacy Policies are privacy preferences expressed by the user about their content disclosure preferences with thier socially connected users.

We define the privacy policies as follows: Definition: A Privacy policy P can be described for user U by

Subject(S): A Set of users socially connected to user U.

Data (D) : A set of data items shared by U.

Action (A) : A set of actions granted by U to S on D.

Condition (C) : A boolean expression which must be satisfied in order to perform the granted actions.

In the above definition, Subject(S) can be user's identities, relations such as family, friend, co-workers, etc. and organizations. Data(D) consists of all the images in the user's profile. Action(A) considers four factors: View, Comment, tags and Download. Lastly the Condition(C) specifies whether the actions are effective or not.

Example 1. Joe wants to allow her friends and family to view and comment on images in the album named "birthday_album" and the image named "cake.jpg"

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

before year 2015.The policy for her privacy preference will be P: [{friend, family}, {birthday_album, cake.jpg},{view ,comment}, (date< 2015)]. allowed.

A3P Architecture

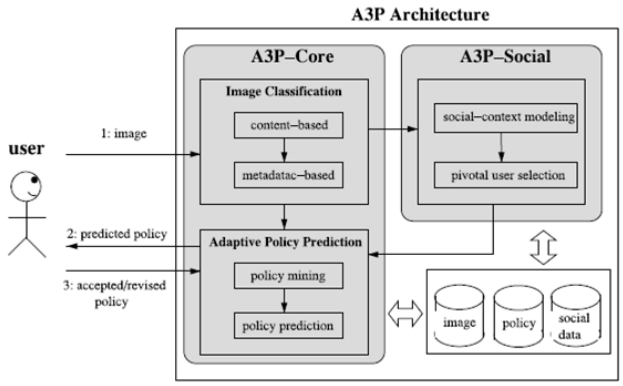
A3P stands for Adaptive Privacy Policy Prediction system which helps users to derive the privacy settings for their images The A3P Architecture consists of followings blocks:

A3P Core.

1. Metadata based Image classification.
2. Adaptive policy prediction.
3. Look-Up Privacy Policies
4. Database

A3P Core classifies the images with the help of the Metadata and also predict the policies depending upon the behaviour of the user.

The Look-up Privacy Policy looks if the image or similar type of image already exists which can be given with similar privacy policies. If similar type of image doesn't exist then it looks for all the policies and lets user choose the policies.



A3P Core

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

1. Metadata based Image Classification
2. Adaptive Policy Prediction

Every image of the user gets classified based on the metadata and then its privacy policies are generalised. With the help of this approach, the policy recommendation becomes easy and more accurate. Based on the Classification based on metadata the policies are applied to the right class of images. Moreover combining the image and classification and policy prediction would enhance the system's dependency.

MODULES:

- System Construction Module
- Content-Based Classification
- Metadata-Based Classification
- Adaptive Policy Prediction

MODULES DESCSRIPTION:

System Construction Module

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 A3Psocial: (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).

Content-Based 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. Such a hierarchical classification gives a higher priority to image content and minimizes the influence of missing tags. Note that it is possible that some images are included in multiple

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

categories as long as they contain the typical content features or metadata of those categories.

Our approach to content-based classification is based on an efficient and yet accurate image similarity approach. 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.

Metadata-Based Classification

The metadata-based classification groups images into subcategories under aforementioned baseline categories. The process consists of three main steps. The first step is to extract keywords from the metadata associated with an image. The metadata considered in our work are tags, captions, and comments. The second step is to derive a representative hypernym (denoted as h) from each metadata vector. The third step is to find a subcategory that an image belongs to. This is an incremental procedure. At the beginning, the first image forms a subcategory as itself and the representative hypernyms of the image becomes the subcategory's representative hypernyms.

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: (i) policy normalization; (ii) policy mining; and (iii) policy prediction.

CONCLUSION

We have studied and approached towards an adaptive privacy policy prediction in this paper that assists users for maintaining the privacy of their uploaded images by automatically recommending privacy policies. This system provides a framework which deduces privacy preference based on the history of the users proclivity. This help user to set hassle free and flexible policy selction.

References

[1] Anna Cinzia Squicciarini, Member, IEEE, Dan Lin, 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] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.

[3] 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

[4] 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.

[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.