Volume No:2, Issue No:2 (July-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

A Novel A3P approach towards Image Privacy on Social Sites

GowrlaVenkatesh
MCA,
CMR College of Engineering and Technology.

Ch. Dayakar Reddy
MCA, M.Tech, MPhile, Ph.D
Professor and Head of Department MCA,
CMR College of Engineering and 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.

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 measuresis 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.

2. 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.

3.SYSTEM ARCHITECTURE

3.1.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.

Volume No:2, Issue No:2 (July-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

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

3.2. 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:

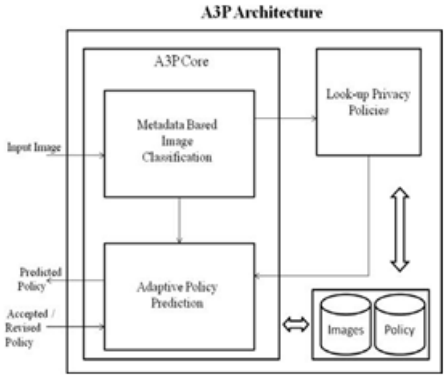
A3P Core.
1.Metadata based Image classification.
2.Adaptive policy prediction.
3.Look-Up Privacy Policies
4.Database
A3P Core classifies the images with the help of the Metadata and also predict the policies depending upon the behaviour of the user.The Look-up Privacy Policy looks if the image or similar 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.
3.3. A3P Core

The A3P Core consist 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.

3.3.1.Metadata Based Image Classification:

As mentioned, the metadata based Image classification groups the images into sub-categories with the help of following three steps.

Step 1 of this process obtains the keywords from the metadata of the image. Tags, Comments and Captions are included in our metadata through which the keywords are obtained. After obtaining the keywords our task is to identify all nouns, verbs and adjectives and store them into a metadata vector such as
Tnoun={t1,t2,t3,…..,tk}, Tverb={t1,t2,t3,…..,tj}, Tadjective={ t1,t2,t3,…..,tl} where k,j and l are the total number of nouns, verbs and adjectives respectively.
Step 2 of this process is to attain a typical hypernym from each metadata vector. The hypernym is denotedby h and first retrieved for every ti. This hypernym can be represented as h={(v1,f1), (v2,f2),….}.Here v denotes as the hypernym and f denotes its frequency. For example, consider a metadata vector T={, "Job", "Promotion","Party"}. With the help of this set we can say that Job and Promotion have the same



hypernym work whereas Party has a hypernymActivity. Hence, we can show the hypernm list as h={(work,2),(Activity,1)}.From this list we select the hypernym with the highest frequency.
Step 3 of this process is to obtain the subcategory in which the image fits in. This step is an incremental procedure in which the first image forms a subcategory and the hypernyms of the image are also allotted to their respective subcategory. For every new incoming image, the distance between these hypernyms and each category is computed and the closest subcategory for that image is discovered.

Volume No:2, Issue No:2 (July-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

3.3.2. Adaptive Policy Prediction:

This part deals with the privacy concerns of the user by deriving the privacy policies for the images. The Adaptive Policy Prediction consists of two following sub-parts:

1.Policy Mining
2.Policy Prediction

Policy mining deals with data mining of policies for similar categorised images and Policy prediction applies prediction algorithm to predict the policies.

Policy Mining: The privacy policies are the privacy preferences expressed by the users. Policy mining deals with mining of these policies by applying different association rules and steps. It follows the order in which a user defines a policy and decides what rights must be given to the images. This hierarchical mining approach starts by looking the popular subjects and their popular actions in the policies and finally for conditions. It can be thoroughly reviewed with the help of following steps.

Step 1 of 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 intrestingness measure i.e., support and confidence which gives the most popular subjects in policies.
Step 2 of 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 of 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:

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.

5.References :

[1] Anna CinziaSquicciarini, Member, IEEE, Dan Lin, SmithaSundareswaran 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.