Secrecy for Images Uploaded by User over Social Media

P. Geethanjally[#1], K. Arunkumar*[2]

[#]PG Scholar, Department of Computer Science and Engineering, RVS College of Engineering and Technology
[1]preethyamirtha@gmail.com

[*]Assistant Professor, Department of Computer Science and Engineering, RVS College of Engineering and Technology
[2]arun1148@gmail.com

***Abstract*—Social media has attracted vast number of users to share their personal information with other users. Privacy becomes a major problem since the information might be shared by 'n' number of users. An Adaptive Privacy Policy Prediction framework has been devised in order to provide security to the information. The framework helps the users to create security measures for the information shared through the social sites. User's privacy preferences such as the role of image, image's metadata are considered as the measures. A policy prediction technique has been generated in order to automatically upload the user images. In addition to this, an image classification framework is used for association of images with similar policies. The main objective of this paper is to provide a substantial method for privacy policy recommendations in order to improve the security of the shared information in the social sites.**

***Index Terms*—privacy policy prediction, social media, A3P framework, policy mining.**

I. INTRODUCTION

Nowadays, social sites play a vital role in sharing information between one another. This type of sharing information might lead to exposure of personal information and privacy vandalism. The exposed information could be misused by malicious users. Privacy settings have to be modified in such a way that the personal images uploaded by the user have to be protected. Recently, investigations on privacy settings have been done by many researchers and it is been analyzed that preserving these measures is very complex and prone-to-error process. Hence, recommendation system is essential for the users since the users need an easy and flexible assistance for providing privacy settings in an easy way. In this paper, an Adaptive Privacy Policy Prediction (A3P) system which focuses on privacy settings experience that uses the automatic generation personalized policies.

The two most important factors that have been considered so as to handle the user uploaded information such as image in A3P that manipulates privacy settings are

1. Maintenance of images uploaded by the user is done with the help of user social activities and individual personal characteristics.
2. Meta data of the images aids in recommending privacy settings.

II. RELATEDWORK

An adaptive Privacy Policy Prediction system has been developed by Anna Cinzia Squicciarini[1]. This system is considered as an automated privacy setting recommendation for system generating personalized policies. User's personal characteristics and images meta data are the measures for the A3P system. The A3P system consists of two components: A3P Core and A3P Social. A3P Core accepts the input as when a user uploads an image. Meta data of the image is used for classification of the images and this is used for association rule data mining algorithm in order to predict the policy. If data is sufficient A3P core does the process, else A3P system will be called to obtain relevant policies. The major disadvantage in this method is the privacy policy generated is inaccurate since the metadata information about the image is not present. The manual creation of metadata log data information leads to inaccurate classification and also privacy desecration. A tool called privacy suites has been proposed by Jonathan Anderson[2]. A privacy suite makes the user to select –suites" of privacy settings. The creation of privacy suites are done with the help of already accessible configuration user interfaces or by exporting them to the abstract format. The privacy suite is disseminated through existing distribution channels to the members of the social sites. The disadvantage of a rich programming language is less understandability for end users. Given a sufficiently high-level language and good coding practice, motivated users should be able to verify a Privacy Suite. The main goal is transparency, which is essential for convincing influential users that it is safe to use. Alessandra Mazzia introduced PViz Comprehension Tool [3], an interface and system that communicates more directly with how users model groups and privacy policies applied to their networks. Using this tool, user can easily understand the visibility of his/her profile as specified by the automatically-constructed behavior, natural sub-groupings of friends, and at different levels of granularity. The user is able to classify and differentiate automatically-constructed groups, the important sub-problem of producing effective group labels is also addressed. PViz is better than other current policy comprehension tools Facebook's Audience View and Custom Settings page. Chen, Chang Proposed a system named SheepDog [3] which inserts photos automatically into appropriate groups and suitable tags are suggested for users on Flickr. They adopt concept detection to predict relevant concepts (tags) of a photo. This system is considered as a reliable system to add photos into popular groups automatically. The main important factor is that suitable tags for photos are recommended and in addition it also provides a user friendly interface such that users find easy in selecting favorite tags for attaching. Adu-Oppong et al proposed the concept of "social circles" i.e. forming clusters of friends [3]. An automatic privacy extraction system which uses the machine learning concepts has been proposed by

Danesiz [5]. Ravichandran et. al [6]investigated about the prediction of the users privacy preferences for location-based data. This was done on the basis of time of the day and location. A recommender system which is known as "YourPrivacyProtector" has been designed by Kambiz Ghazinour[7] is used for recognizing the social net behavior and it also provides recommendations for privacy options. To create personal profile, user's interests and user's privacy settings are used. This system enables the users to observe their privacy settings on their social network profile, and also it helps in monitoring and as well as detecting the privacy risks. Klemperer et al. [8] does an analysis on keywords, captions and the way of using it for tagging user's photos. In addition to it, he also investigated the efficient ways of using tags and captions and how to maintain access control policies.

III. SYSTEM ARCHITECTURE

A. A3P Framework

Privacy policy is defined as the settings done by the user in order to provide the security for the information uploaded in the social sites. Various notations used in privacy policy are

P : Privacy Policy
U : Individual User
S : Subject (collection of users connected to an individual user U)
D : A data item shared by U.
A : Set of actions granted by U to S on D.
C : A boolean expression which must be satisfied in order to perform the appointed actions. It is termed as condition.

Subject(S) refers to the socially connected people on websites like relations such as family, friend, co-workers, etc. and organizations. Data (D) is the collection of image uploaded by user till date. Action (A) comprises of four factors: View, Comment, Tags and Download. Condition(C) specifies whether the actions are effective or not. An example policy is stated as given below.

Example 1:

Alice would like to allow her friends and family to comment and tag images in the album named "convocation_album" and the image named "degree.jpg" before year 2016. Her privacy preferences can be stated by the following policy:

P :[{ friends, family}, {convocation_album, degree.jpg}, {comment, tag}, (date < 2016)].

A3P (Adaptive Privacy Policy Prediction) is a framework used for defining new privacy preferences policies for users and to make the experience flexible and secure at the time. The A3P Architecture consists of followings components:

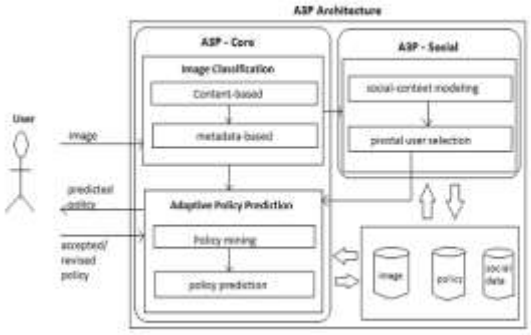

Fig. 1 System Architecture

1. A3P Core.
   - Metadata based Image classification.
   - Adaptive policy prediction
2. Look-Up Privacy Policies
3. Database

Classification of images is done with the help of Meta data and a new predicted policy based on the user behavior is done in A3P Core. The Look-up Privacy Policy component issues the same policy predicted if the required image is present in the database. Otherwise, the image is stored as new data for further help in policy prediction.

A3P Core: The A3P Core consists of two major components.

i. Metadata based Image Classification
ii. Adaptive Policy Prediction

Due to the metadata based classification component, the policy recommendation becomes easier and accurate since a comparison and classification is done on the user uploaded images. This metadata based image classification plays a vital role in providing better and efficient policies for users.

B. Metadata Based Image Classification

It is divided into sub-categories with the help of following three steps.

Step 1: Extraction of keywords from the metadata of the image. Keywords refer to Tags, captions and comments. A metadata vector is created and it contains nouns, verbs, adjectives. A metadata vector is represented as V = {α, β, γ} where α= $\{n_1, n_2, \ldots n_i\}$, β= $\{v_1,v_2,v_3,\ldots v_j\}$ and γ= $\{a_1,a_2,a_3,\ldots a_k\}$ where i,j,k represents the total number of nouns, verbs and adjectives.

Step 2: A similar hypernym from each vector is created. The hypernym is denoted by 'h' and first retrieved for every V. This hypernym can be represented as "h={(h1,f1), (h2,f2),….}".Here 'h' are hypernyms and 'f' is for frequency. For example consider a metadata vector V= { "cat","dog"," walk"}.By this set, it is easily understood that cat and dog are

related with same hypernym "pet animals" whereas "walk" is an activity. Hence it can be denoted as h= {("pet animals", 2), (activity, 1)}. Select the hypernym with the maximum frequency.

Step 3: Identify the sub category in which the image file fits. The first image forms a subcategory and the hypernyms of the image are also assigned to their respective subcategory. A subcategory for an image is computed by identifying the proximity of these hypernyms.

C. Adaptive Policy Prediction:

This process deals with the privacy concerns of the user by deriving the privacy policies for the images. The Adaptive Policy Prediction consists of two phases

i. Policy Mining
ii. Policy Prediction

Mining of policies for images with similar categories are done in the policy mining phase. The second phase deals with the prediction algorithm to predict the policies.

i. Policy Mining: The privacy policies are the privacy preferences expressed by the users. Mining is done by applying association rules and methodologies. A sequence is followed so that the user will be able to identify the type of policy and the rights that are applicable to images. This hierarchical mining approach starts the process by analyzing the important subjects and their popular actions in the policies and at last goes for the conditions. It can be approached with the help of following steps. The first step is to focus on association rule and its mining on the subject components of the image and its policies. With the association rule mining, one can write the best rules according to one of the interestingness measure i.e., support and confidence giving the most popular subjects in policies. Step 2 of this process applies the rules on the action components. Similar to the first step the best rules are selected which gives the combinations of action in policies. In Step 3, mining is done on the condition component in each policy set. The rules giving the best outcomes are selected which gives us a set of attributes which frequently appear in policies.

ii. Policy Prediction: This is used to identify the best approach for the user on the basis of strictness level. The strictness level is denoted by an integer. Its value must be least to obtain high strictness. The strictness can be identified by major level and coverage rate. To calculate the major level, operations on subject and action in a policy is used and the coverage rate is resolved with the help of condition. Different range values are assigned based on the strictness to the combinations and for data with multiple combinations the lowest rate is selected. It provides a fine-grained strictness level which adjusts the major level obtained earlier. For example a manager has five assistants and among them two of them are from the sane state. Hence, if a policy has to be framed based on this, then it can be written as "assistants"=other state. If it is applied, then the coverage rate can be calculated as (3/5)=0.6. Hence, the restricted on the image is less if the coverage rate value is high.

IV. CONCLUSION

This paper has discussed about the adaptive privacy policy prediction. This framework is used for assisting users in order to maintain the privacy of their uploaded images with the help of automatically generated privacy policies. This system provides a framework which deduces privacy preference based on the history of the users penchant. Thus it aids the user to select the policy in an easy way.

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] Alessandra Mazzia Kristen LeFevre and Eytan Adar,"The PViz Comprehension Tool for Social Network Privacy Settings", Tech. rep., University of Michigan, 2011.

[4] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P.Tsang, "Social circles: Tackling privacy in social networks,"in Proc. Symp. sable Privacy Security, 2008.

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

[6] 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.

[7] Kambiz Ghazinour, Stan Matwin and Marina Sokolova,"Your privacy protector: A Recommender System For Privacy Settings In Social Networks", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 4, August 2013.

[8] Peter F. Klemperer, Yuan Liang, Michelle L. Mazurek, "Tag, You Can See It! Using Tags for Access Control in Photo Sharing", Conference on Human Factors in Computing Systems, May 2012.

[9] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt,"Providing access control to online photo albums based on tags and linked data", in Proc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp.

