Secure Privacy Policy for User Uploaded Images On Social/Content Sharing Sites

#1Ms.Gaikwad S.S, #2 Prof.Amrit Priyadarshi

*gaikwad.swati11@gmail.com
amritpriyadarshi@gmail.com

#12Department Of Information Technology, DGOIFOE, Daund,Pune,India

ABSTRACT

Usage of social media’s increased considerably in today world which enables the user to share their personal information like images with the other. This improved technology leads to privacy violation where the users are sharing the large volumes of images across more number of peoples. To provide security for the information, automated annotation of images are introduced which aims to create the meta data information about the images by using the novel approach called Semantic annotated Markovian Semantic Indexing(SMSI) for retrieving the images. 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. Over time, the generated policies will follow the evolution of users’ privacy attitude.

Keywords: Social media; Content sharing sites; Privacy; Meta data

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+,Flickor,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 students 2012 graduation ceremony, for example. It could be shared within a Google+ circle or Flicker group, but may unnecessarily expose the students'Apog family members and other friends. 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

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. For amount of shared information this process can be tedious and error-prone. So, acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings.

DISADVANTAGES OF EXISTING SYSTEM

1. Sharing images within online content sharing sites, therefore may quickly lead to unwanted disclosure and privacy violations.
2. 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 personal information.

LITERATURE SURVEY

“Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites” Anna Cinzia Squicciarini [1]. It developed an A3P system, a free privacy settings system by automatically generating personalized policies. The A3P system handles user uploaded images based on the person’s personal characteristics and images content and metadata. Two components are present in A3P system: A3P Core and A3P Social. 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. The disadvantage is inaccurate privacy policy generation in case of the absence of metadata information about the images. Also manual creation of metadata log data information leads to inaccurate classification and also violation privacy.

“Privacy suites: Shared privacy for social networks”, Jonathan, Anderson [2]. This paper proposed a paradigm called Privacy Suites in which users give privacy settings by choosing suits. Expert can create a privacy suite by privacy programming. It could also be created by directly through existing configuration UIs or exporting them to the abstract format. Distribution channels are used to distribute privacy suite to the social sites members. End users are unable to understand rich programming language. Activated users can verify a Privacy Suite by use of high-level language and good coding practices. Transparency is the goal, which ensures users to safe to use.

“Social circles: Tackling privacy in social networks”, Adu-Oppong [3]. It uses concept of social circles to develop privacy settings. It protect personal information through web based solution. Different technique like Social Circles Finder, automatically generates the friend’s list. Identify the social circles of the subject, not showing them. Identify social circle of a person, identifies the potency of relationship and so it is providing a significant categorization of friends for setting privacy policies. Asked questions about their willingness to share a piece of their personal information, based on the answers finds the visual graph of users [15].

“Social circles: Yourprivacyprotector: A Recommender System For Privacy Settings In Social Networks”, Kambiz Ghazinour [4]. This paper advice system known as YourPrivacyProtector that grasp the privacy settings social net behavior and suggest sensible privacy options. Different parameters has used to constructs the personal profile of the user that has user’s personal profile, User’s interests and User’s privacy settings on photo albums. So learned automatically a given profile of users and assigned the privacy options. Users could see their current privacy settings on their social network profile, namely Facebook, and monitors and detects the possible privacy risks. Adopts the necessary privacysettings, based on the risks.

“Social circles: The PViz Comprehension Tool for Social Network Privacy Settings”, Alessandra Mazzia [5]. This paper introduced PViz Comprehension Tool an interface that shows how users model groups and privacy policies used to their networks. User are able to understand the visibility of her profile according to automatically-constructed, natural sub-groupings of friends, and at different levels of granularity. Because of this, we also address the important sub-problem of producing effective group labels. PViz is better than other current policy comprehension tools Facebook’s Audience View and Custom Settings page.

“Tag, You Can See It! Using Tags for Access Control in Photo Sharing”, Peter F. Klemperer [6]. It shared in the social media sites. System creates access-control policies from photo management tags. Incorporated every photo with an access grid to map the photo with the participant’s friends. Classify photo tags as organizational or communicative based on the user needs. The participants can select a suitable preference and access the information. Different limitations to our study design are our results are limited by the participants we recruited and the photos they provided. Set of limitations concerns our use of machine generated access-control rules. When tagging for access control the algorithm has no access to the context and meaning of tags and no insight into the policy the participant intended. As a result, some rules appeared strange or arbitrary to the participants, potentially driving them toward explicit policy-based tags like “private” and “public”. Ching-man Au Yeung propose a access control system based on a decentralised authentication protocol [7], descriptive tags and linked data of social networks in the Semantic Web. Photos that are shared in one or more photo sharing sites created expressive policies for that photos and specify access control rules based on open linked data provided by other parties.

“Privacy-Aware Image Classification and Search”, Sergej Zerr[8]. I this technique propose a automatically detecting private images, and to enable privacy-oriented image search. It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game. In this the selected image features (edges, faces, color histograms) which can help discriminate between natural and man-made objects/scenes (the EDCV feature) that can indicate the presence or absence of particular objects (SIFT). It combines textual metadata images with variety of visual features to provide security policies.

PROPOSED SYSTEM

1. 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:
a. 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.

b. 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

1. 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.

2. We design the interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice.

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.

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.


