Privacy Policy Inference of User-Uploaded Images on social network

Prof. Bhadkumbhe S.M.[1], Hatkar V.S.[2], Patil N.M.[3], Pawar A.A.[4] Salunke S.K.[5]

[1] *Professor, Computer Engineering, P.D.E.A.'s COE Manjari(Bk), Maharastra, India*
[2] *Student, Computer Engineering, P.D.E.A.'s COE Manjari(Bk), Maharastra, India*
[3] *Student, Computer Engineering, P.D.E.A.'s COE Manjari(Bk), Maharastra, India*
[4] *Student, Computer Engineering, P.D.E.A.'s COE Manjari(Bk), Maharastra, India*
[5] *Student, Computer Engineering, P.D.E.A.'s COE Manjari(Bk), Maharastra, India*

ABSTRACT

Social Network is an emerging e-service for content sharing sites (CSS).With the increasing large no. of images users share through social sites, has maintaining privacy and protection has become a major problem, as demonstrated by a recent wave of incidents where users carelessly shared personal information. Social Networking Sites (SNS) such as Facebook and MySpace have engage millions of users because of their ability to connect individuals by social graphs and status. In light of these events, the need of tools and protector to help users control access to their shared image content is likely. Toward addressing this need, we propose an Adaptive Privacy Policy Prediction (A3P) system and NLP processing 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 novel approach of grouping friends to improve the privacy policy also 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. 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. 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. We provide the results of our extensive evaluation over 6,000 policies, which demonstrate the effectiveness of our system, with prediction accuracies over 80 percent

Keyword: - • *Online information services , Web-based services,* • *Image Processing, and* • *NLP etc..*

1. INTRODUCTION

Images are shared extensively now 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. Social Networking (SN) is an improving technology with hundreds of millions of people participating in swapping their content through text, media like image, audio, video, etc. Social media (SM) become one of the most important parts of our daily life as it allows us to communicate with a group of people. It assists an exterior of self-expression for users, and assists them to entertain and exchange content with other users through social media's e-service. Some of the social networks like Friendster.com, Tagged.com, Xanga.com, Live Journal, MySpace, Facebook, Twitter and LinkedIn have developed on the Internet over the past several years. It provides a content sharing mechanism and connects people across the world. Users of social media can define a personal profile and modify it as they wish. This feature is allowed by the SM. Through this SM, users may engage with each other for various purposes like business, leisure, and knowledge sharing. People use social networks to get in touch with further people, and create and contribute content that includes personal information, images, and videos. The service providers have admission to the content presented by their users and have the right to collect data and share them to unauthorized users. A very familiar service provided in SN is to produce proposition for finding new friends, groups, and events using mutual filtering techniques. The

success of the SN based on the number of users it attracts, and cheering users to add more users to their circle and to share data with other users in the SN. So the information will go across the world [1]. End users are nevertheless often not aware of the size or nature of the spectators accessing their data and the sense of understanding created by organism among digital friends often leads to disclosures that may not be suitable in a public forum. Due to such an open accessibility of exposed data in SN, the users face a number of security and privacy risks.

In spite of the fact that content sharing represents one of the important features of existing Social Network sites, Social Networks yet do not sustain any mechanism for collaborative execution of privacy settings for shared content [2]. Social Networking sites are used by a huge number of users all over the world. It provides different features to the customers like chatting, posting comments, image sharing, video chatting etc. Images are now one of the key enablers of user's connectivity. Sharing takes place both among previously established groups of known people or social circles (e.g., Google+, Flickr 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 [2]. Consider a photo of a student's2012 graduation ceremony, for example. It could be shared within a Google+ circle or Flickr group, but may unnecessarily expose the students. Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations [3], [4]. 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], [2], [4]. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

1.1 NLP:

A typical application is to scan a set of documents written in a natural language and either model the document set for predictive classification purposes or populate a database or search index with the information extracted.

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. RELATED WORK

Our work is related to works on privacy setting configuration in social sites, recommendation systems, and privacy analysis of online images.

3.1 Privacy Setting Configuration

Privacy suites which recommend to users a suite of privacy settings that "expert" users or other trusted friends have already set, so that normal users can either directly choose a setting or only need to do minor modification. A machine-learning based approach to automatically extract privacy settings from the social context within which the data is produced. The aforementioned approaches focus on deriving policy settings for only traits, so they mainly consider social context such as one's friend list. While interesting, they may not be sufficient to address challenges brought by image files for which privacy may vary substantially not just because of social context but also due to the actual image content.

In addition, there is a large body of work on image content analysis, for classification and interpretation

3.2 Recommendation Systems

To some existing recommendation systems which employ machine learning techniques. a system named SheepDog to automatically insert photos into appropriate groups and recommend suitable tags for users on Flickr. They characterize images through three types of features: visual features, user generated text tags, and social interaction, from which they recommend the most likely groups for a given image.

4. A3P FRAMEWORK

Our work is related to works on privacy setting configuration in social sites, recommendation systems, and privacy analysis of online images.

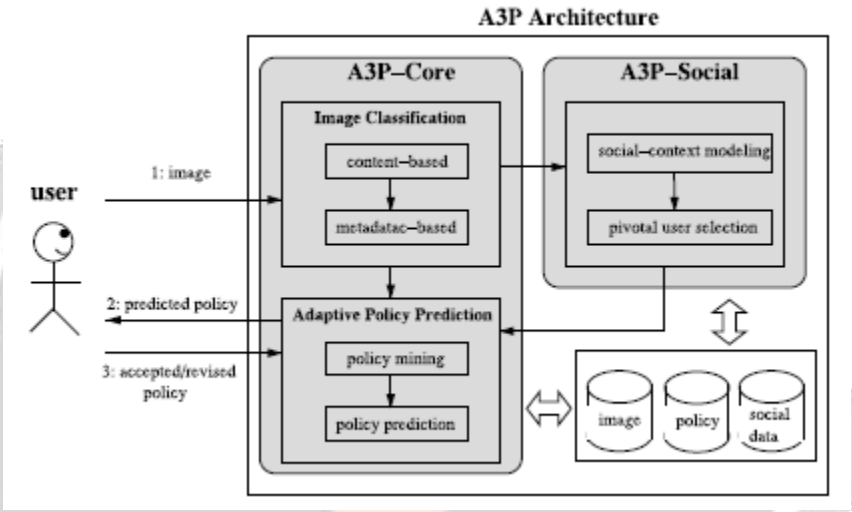

Fig 1. A3P Framework

4.1 Preliminary Notions

We define privacy policies according to Definition 1. Our policies are inspired by popular content sharing sites (i.e., Facebook, Picasa, Flickr), although the actual implementation depends on the specific content-management site Structure and implementation.
A privacy policy P of user u consists of the following components:

Subject (S): A set of users socially connected to 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.

4.2 System Overview

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

5 Relevant Mathematics Associated with the Project

Module 1) User account Validation and Forgot Password

Let S1 be a set of parameters for Proper user validation

S1= User Validation, Image Select

If user want to create the Account

then user proper validation and selected image completely then

Login to user account

If already account is created then only checks the user name and password

If user forgot the password then user wants to select the image,

Then system sends the OTP and get changed password.

Module 2)Image Processing

Lets S2 be a set of user data

S2=Image File

Where,

Image File = user upload image

The image contents check using the NLP , Image Processing Algorithm

If image verify

Then image upload in that particular group

If image content in warning content

Then block the image if user upload this file then system sends the OTP.

6. CONCLUSIONS

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.

And also 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 selection.

7. ACKNOWLEDGEMENT

In our endeavor to achieve the success in completing project report of stage 1 on Privacy Policy Inference of User-Uploaded Images on social network in the Final Year Engineering in Computer. We take this opportunity to express our deep sense of gratitude to our guide respected Prof. S. M. Bhadkumbhe, for his valuable guidance and kind co-operation throughout the period of work has undertaken which has been instrumental in success of project stage 1.

I especially thankful to our project Incharge Prof.R.B.Rathod Sir, he have also guided us much for preparation of each and every project work. We also very thankful to our respected H.O.D. Dr. R.V.Patil Sir, for providing us with adequate facilities, ways and means by which I was able to complete this project report stage 1. We would also like to thank our respected Principal Dr. D.A.Kambale Sir who creates a healthy environment for all of us to learn in best possible way. We express our thankfulness to all teachers and staff of computer department for timely help in course of project report stage 1.

Finally, special thanks to my friends, family members and all others those unseen people across the internet for maintaining sources on the internet that helped us in the successful completion of this work

8. 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. Deng, A. C. Berg, K. Li, and L. Fei-Fei, "What does classifying more than 10,000 image categories tell us?" in Proc. 11th Eur. Conf. Comput. Vis.: Part V, 2010, pp. 71–84. [Online]. Available:

[3]. 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.

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

[5]. EU IST MUSIC project, Self-Adapting Applications for Mobile Users in Ubiquitous Computing Environments, http://www.ist-music.eu, 2008.

[6]. K. Verlaenen, B. De Win, and W. Joosen, "Policy Analysis Using a Hybrid Semantic Reasoning Engine", Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY '07). IEEE Computer Society, pp. 193-200, 2007.