ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Privacy Policy for User Uploaded Images

Anjali More[1], Pooja Sakunde[2], Gandhali Deshpande[3], Tejas Jatkar[4,] Rajesh Bharti[5]

Student, Department of Computer Engineering, DYPIET, Pimpri Pune, Savitribai Phule Pune University Pune India[1,2,3,4]

Professor, Department of Computer Engineering, DYPIET, Pimpri Pune, Savitribai Phule Pune University Pune India[5]

ABSTRACT: Social Network is an emerging E-service for content sharing sites (CSS). It is emerging service which provides a reliable communication, through this communication a new attack ground for data hackers; they can easily misuses the data through these media. Some users over CSS affects users privacy on their personal contents, where some users keep on sending unwanted comments and messages by taking advantage of the users' inherent trust in their relationship network. 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. We provide the results of our extensive evaluation over 5,000 policies, which demonstrate the effectiveness of our system, with prediction accuracies over 90 percent.

KEYWORDS: Social media; content sharing sites, Privacy, Meta data, CSS, APP.

I. INTRODUCTION

Social Networking (SN) is one of the improving technological with hundreds of millions of people participating to 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 providing E-Service. Some of the Social media are 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 remote the people across the world. Users of social media can define a personal profile and modify it as they wish this features allows by the SM. Through this SM users may engage with each other for various purposes, with 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 present by their users and have the right to progression collecteddata and share them to unauthorized. 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 goes 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. Such an open accessibility of data exposes in SN, the users obtain 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 executive 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 users' connectivity.Sharing takes place both among previouslyestablished groups of known people or social circles (e.g., Google+, Flickr or Picasa), and also increasingly withpeople outside the users social circles, for purposes ofsocial discovery-to help them identify new peers andlearn about peers interests and social surroundings.However,

DOI: 10.15680/IJIRCCE.2016. 0405120

semantically rich images may reveal contentsensitiveinformation [2]. Consider a photo of a student's2012 graduationceremony, for example. It could beshared within a Google+ circle or Flickr group, but mayunnecessarily 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 forother 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.

II. RELATED WORK

Consider a photo of a student's 2012 graduation ceremony, for example. It could be shared within a Google+ circle or Flickr group, but may unnecessarily expose the student's 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 socialenvironment and lead to abuse of one's personal information.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 privacysettings. 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. However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images, due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed.Our work is related to some existing recommendation systems which employ machine learning techniques. Chen et al. [7] proposed a system named Sheep Dog to automatically insert photos into appropriate groups and recommend suitable tags for users on Flickr. They adopt concept detection to predict relevant concepts (tags) of a photo. Choudhury et al. [10] proposed a recommendation framework to connect image content with communities in online social media. 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. Similarly, Yu et al. [42] proposed an automated recommendation system for a user's images to suggest suitable photo-sharing groups.Usage of social media's increased noticeably in today world which facilitate the user to distribute theirpersonal information like images with the other. This enhanced technology leads to privacy disobedience where theusers are allocation the large volumes of images across additional number of peoples. To provide security for theinformation, mechanical explanation of images are introduced which aims to create the meta data information about theimages by using the novel approach called Semantic interpret Markovian Semantic Indexing(SMSI) for repossess theimages [1]. The proposed system automatically interpret the images using hidden Markov model and features areextorted by using color histogram and Scale-invariant feature transform (or SIFT) descriptor method. After interpretthese images, semantic retrieval of images can be done by using Natural Language giving out tool namely Word Netfor measuring semantic comparison of annotated images in the database. Experimental results make available enhancedretrieval performance when evaluate with the existing system.An approach that produces access-control policies from photo management tags. Every photo is included with an access network for mapping the photo with the participant's friends. The contributor can choose apposite preference and access the data. Photo tags can be classified as managerial or unrestrained based on the user needs. There are several significant limitations to our study design. First, our outcomes are limited by the participants we conscript and the photos they offered. A second set of limitations apprehension our use of machine generated access-control rules. The algorithm has no admittance to the context and significance of tags and no approaching into the policy the contestant proposed when tagging for access control. As an outcome, some rules become visible strange or random to the contributor, potentially pouring them in the direction of explicit policy-based tags like "private" and "public.The A3P system levers user uploaded images based on the person's individual characteristics and images content and metadata. The A3P system consists of two components: A3P Core and A3P Social.

III. OBJECTIVE

1. Maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information.
2. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need, we propose an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images.
3. 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.
4. Our purpose is related to works on privacy setting configuration in social sites, recommendation systems, and privacy analysis of online images.

IV. SYSTEM ARCHITECTURE

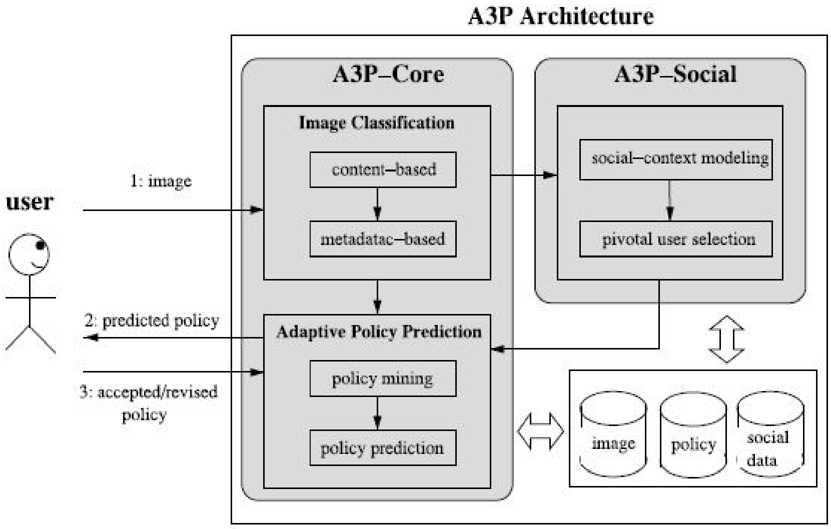

Figure No. 01 System Architecture

Explanation

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:

1. 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.

2. The role of image's content and metadata. In general, similar images often incur similar privacy preferences, especially when people appear in the images.

V. MODIFIED ARCHITECTURE

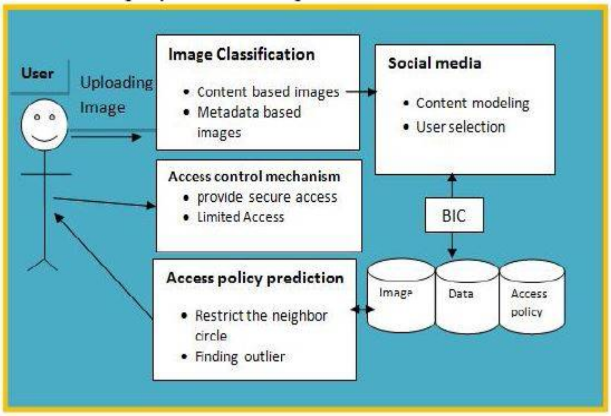

Figure No. 02 Modified Architecture

Architecture Explanation

Some users over CSS influence user's privacy on their private contents, where some users keep on distribution superfluous comments and messages by attractive advantage of the users' intrinsic trust in their connection network. The overall architecture of the proposed work has given in figure 1.0. This paper switches the most widespread issues and threats objective different CSS freshly. In CSS privacy is frequently a key apprehension by the users. Because millions of people are willing to interrelate with others, it is also a new harass ground for image misuses. They are dispersion the images and contents. This paper will demonstrate and argue the most widespread issues and threats targeting different CSS today. And finally finds the just the thing privacy policy scheme for that privacy. This proposition a privacy policy forecast and access boundaries along with overcrowding scheme for social sites using data mining techniques. This helps to detect and defend distrustful activates, which violates user's privacy in CSS by making an allowance for the following parameters, i) Text annotation, which emerge in the uploaded contents. ii) Image and policy descriptions iii) Detection of superfluous commends and. To perform this, the system utilizes APP (Access Policy Prediction) and Access control mechanism by applying BIC algorithm (Bayesian Information Criterion).

VI. MODULE IMPLEMENTATION

A3P-CORE

There are two major components in A3P-core: (i) Image classification and (ii) Adaptive policy prediction. For each user, his/her images are first classified based on content and metadata. Then, privacy policies of each category of images are analyzed for the policy prediction. Adopting a two-stage approach is more suitable for policy recommendation than applying the common one-stage data mining approaches to mine both image features and policies together. Recall that when a user uploads a new image, the user is waiting for a recommended policy. The two-stage approach allows the system to employ the first stage to classify the new image and find the candidate sets of images for the subsequent policy recommendation. As for the one-stage mining approach, it would not be able to locate the right class of the new image because its classification criteria need both image features and policies whereas the policies of the new image are not available yet. Moreover, combining both image features and policies into a single classifier would lead to a system which is very dependent to the specific syntax of the policy. If a change in the supported policies were to be introduced, the whole learning model would need to change.

Image 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 categories as long as they contain the typical content features or metadata of those categories. The content-based classification creates two categories: “landscape” and “kid”. Images C, D, E and F are included in both categories as they show kids playing outdoor which satisfy the two themes: “landscape” and “kid”. These two categories are further divided into subcategories based on tags associated with the images. As a result, we obtain two subcategories under each theme respectively. Notice that image G is not shown in any subcategory as it does not have any tag; image A shows up in both subcategories because it has tags indicating both “beach” and “wood”.

Policy Mining

We propose a hierarchical mining approach for policy mining. Our approach leverages association rule mining techniques to discover popular patterns in policies. Policy mining is carried out within the same category of the new image because images in the same category are more likely under the similar level of privacy protection. The basic idea of the hierarchical mining is to follow a natural order in which a user defines a policy. Given an image, a user usually first decides who can access the image, then thinks about what specific access rights (e.g., view only or download) should be given, and finally refine the access conditions such as setting the expiration date. Correspondingly, the hierarchical mining first look for popular subjects defined by the user, then look for popular actions in the policies containing the popular subjects, and finally for popular conditions in the policies containing both popular subjects and conditions.

A3P-SOCIAL

The A3P-social employs a multi-criteria inference mechanism that generates representative policies by leveraging key information related to the user’s social context and his general attitude toward privacy. As mentioned earlier, A3Psocial will be invoked by the A3P-core in two scenarios. One is when the user is a newbie of a site, and does not have enough images stored for the A3P-core to infer meaningful and customized policies. The other is when the system notices significant changes of privacy trend in the user’s social circle, which may be of interest for the user to possibly adjust his/her privacy settings accordingly. In what follows, we first present the types of social context considered by A3P-Social, and then present the policy recommendation process.

We have proposed an Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacy policysettings 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.

VI. EXPERIMENTAL SETUP

These shows the diverse between existing and the proposed system (see figure 3.0). In the proposed system the access of the pages were limited when compared to existing system. Access control is by provided that access rights in a SN are limited to few basic constitutional rights, such as read, write and play for media content. This based type of approach which generates access-control policies from photo administration tags. Every photo is integrated with an access grid for mapping the photo with the participant’s friends. The contestant can select a suitable partiality and access the information. Photo tags can be categorized as directorial or forthcoming based on the user needs.

DOI: 10.15680/IJIRCCE.2016. 0405120

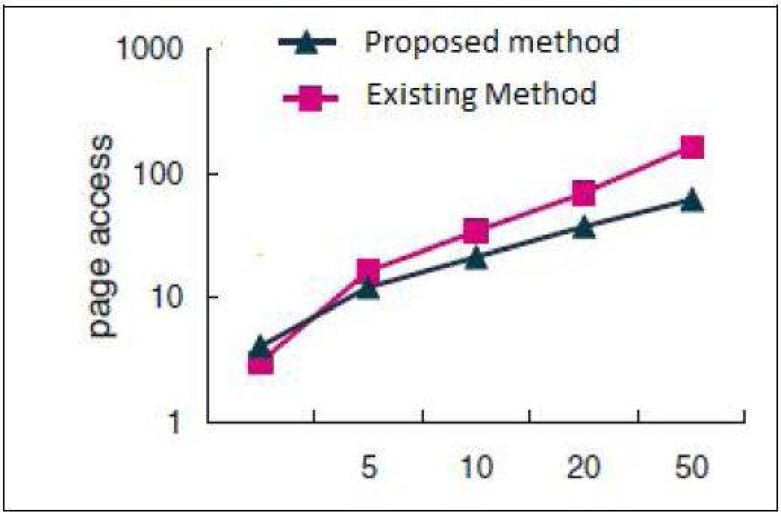

Figure No. 03 Comparison of Existing g and proposed System

Accessing the personal data in E-service make available an information distribution diagonally the world and at the same time it not working the privacy of the user data. Access policy is for retrieving the data or image in thenetwork. By this kind of right of entry privacy may loss. For this problem the user of the social media compute the normalized and prejudiced average of the ratings of the users in the district. User have to confine the neighbor circle so un-wanted may not influence the data [13, 14]. User have to envisage the neighbor circle and provide a limited admission technique they have to choose 1) what information one disclose about oneself, and (2)who can access that information. Fundamentally, when the data is collected or investigate without the knowledge or consent of its owner, privacy is violated.

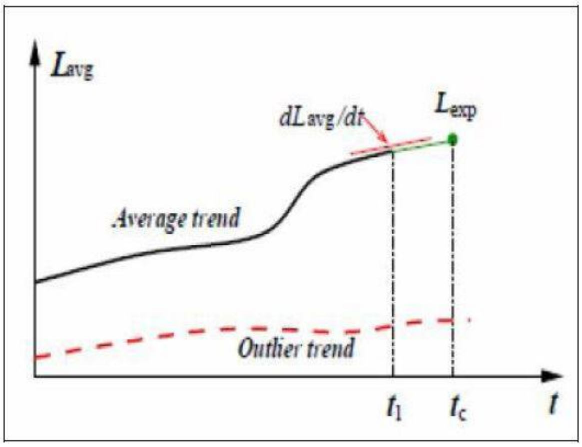

Figure No. 03 Access Policy Prediction

VII. CONCLUSION

This paper describes privacy policy techniques for user uploaded data images in various content sharing sites. Based on the user social behaviour and the user uploaded image the privacy policy can apply. A3P system in used, which provide users easy and properly, configured privacy setting for their uploaded image. By using this we can easily prevent unwanted discloser and privacy violations. Unwanted discloser may lead to misuse of one’s personal information .users automate the privacy policy settings for their uploaded images with the help of adaptive privacy policy prediction

(A3P). Based on the information available for a given user the A3P system provides a comprehensive framework to infer privacy preferences. A3P system is a practical tool. An improvement over current approaches to privacy is offer by A3P.

REFERENCES

[1] A. Acquisti and R. Gross, “Imagined communities: Awareness, information sharing, and privacy on the facebook,” in Proc. 6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006, pp. 36–58.
[2] R. Agrawal and R. Srikant,“Fast algorithms for mining association rules in large databases,” in Proc. 20th Int. Conf. Very Large Data Bases, 1994, pp. 487–499.
[3] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, “Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing,” in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 357–366.
[4] M. Ames and M. Naaman, “Why we tag: Motivations for annotation in mobile and online media,” in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 971–980.
[5] A. Besmer and H. Lipford, “Tagged photos: Concerns, perceptions, and protections,” in Proc. 27th Int. Conf. Extended Abstracts Human Factors Comput. Syst., 2009, pp. 4585–4590.
[6] D. G. Altman and J. M. Bland ,“Multiple significance tests: The bonferroni method,” Brit. Med. J., vol. 310, no. 6973, 1995.
[7] J. Bonneau, J. Anderson, and L. Church, “Privacy suites: Shared privacy for social networks,” in Proc. Symp. Usable Privacy Security, 2009.
[8] 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.
[9] H.-M. Chen, M.-H.Chang, P.-C.Chang, M.-C.Tien, W. H. Hsu, and J.-L. Wu, “Sheepdog: Group and tag recommendation for flickr photos by automatic search-based learning,” in Proc. 16th ACM Int. Conf. Multimedia, 2008, pp. 737–740.