Adaptive Privacy Policy Prediction of User Uploaded Images on Content Sharing Sites

Mr. V SUDHARSHAN
Associate Professor & HoD
Department Of CSE,
Khammam Institute of Technology & Sciences
Khammam, Telangana, India.

SK. NAGASAIDULU
Assistant Professor,
Department Of CSE,
Khammam Institute of Technology & Sciences
Khammam, Telangana, India.

BOJJA KALPANA
M.Tech Student,
Department Of CSE,
Khammam Institute of Technology & Sciences
Khammam, Telangana, 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. To achieve this privacy settings for the people images we are using Adaptive Privacy Policy Prediction system. The proposed system automatically annotates the images using hidden Markov model and features are extracted by using color histogram and Scale-invariant feature transform (or SIFT) descriptor method. After annotating these images, semantic retrieval of images can be done by using Natural Language processing tool namely Word Net for measuring semantic similarity of annotated images in the database. Experimental result provides better retrieval performance when compare with the existing system.**

Keywords: **Semantic Annotated Markova Semantic Indexing, Hidden Markov Model, Hidden Markov Model.**

I. INTRODUCTION

Social media is the two way communication in Web 2.0 and it means to communicate, share, and interact with an individual or with a large audience. Social networking websites are the most famous websites on the Internet and millions of people use them every day to engage and connect with other people. Twitter, Facebook, LinkedIn and Google Plus seems to be the most popular Social networking websites on the Internet. Today, for every single piece of content shared on sites like Face book—every wall post, photo, status update, and video—the up loader must decide which of his friends, group members, and other Facebook users should be able to access the content. As a result, the issue of privacy on sites like Face book has received significant attention in both the research community and the mainstream media. Our goal is to improve the set of privacy controls and defaults, but we are limited by the fact that there has been no in- depth study of users' privacy settings on sites like Face book. While significant privacy violations and mismatched user expectations are likely to exist, the extent to which such privacy violations occur has yet to be quantified. 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. 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. 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 proposed A3P system is comprised of two main building blocks: A3P-Social and A3P-Core. 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. We design the inter-action flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice. To assess the practical value of our approach, we built a system prototype and performed an extensive experimental evaluation.

We collected and tested over 5,500 real policies generated by more than 160 users. Our experimental results demonstrate both efficiency and high prediction accuracy of our system. In this work, we present an overhauled version of A3P, which includes an extended policy prediction algorithm in A3P-core (that is nowparameterized based on user groups and also factors in possible outliers), and a new A3P-social module that develops the notion of social context to refine and extend the prediction power of our system. We also conduct additional experiments with a new data set collecting over 1,400 images and corresponding policies, and we extend our analysis of the empirical results to unveil more insights of our system's performance.

II. RELATED WORK

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

A. Privacy Setting Configuration

Danezis proposed a machine-learning based approach to automatically extract privacy settings from the social context within which the data is produced. Adu-Oppong et al. develop privacy settings based on a concept of ―Social Circles‖ which consist of clusters of friends formed by partitioning users' friend lists. Fang et al. proposed a privacy wizard to help users grant privileges to their friends. The wizard asks users to first assign privacy labels to selected friends, and then uses this as input to construct a classifier which classifies friends based on their profiles and automatically assign privacy labels to the unlabeled friends.

Search: When you first use Search on your phone, you are asked whether or not you'd like to allow Search to use your location information. In Android, the browser settings page allows you to turn off browser location entirely or clear the sites that you have previously given permission to access your location. On other phones (BlackBerry or iPhone, for example) you can disable location through the options in the app itself.

Maps: Google Maps makes use of your web browser's geolocation feature to determine your location. Google Maps accesses your location from your browser and can only do so with your explicit consent. The first time you use the My Location feature, your browser will ask whether you're happy to share your location with Google Maps. If you deny this, your location is not shared with Google Maps and the My Location feature will be deactivated.

Latitude: Google Latitude gives you control over how much or how little location information you want to share with whomever you choose. Before someone can view your location, you must either send the person a location request by adding them as a friend or accept their location request and choose to share back your location. You can sign out of and turn off Google Latitude to stop sharing your location with friends at any time from the privacy menu. For more information about how to set your privacy settings on Latitude, check out this short video.

Android devices: On Android devices you can turn off geo location for all apps and websites. Visit the ―Location and Security‖ or ―Location services‖ menu under Settings to do this. Once turned off, if an app or website wishes to access location information, it will ask you to change your settings or work without this information.

B. Recommendation Systems Chen et al. proposed a system named SheepDog to automatically insert photos into appropriate groups and recommend suitable tags for users on Flicker. They adopt concept detection to predict relevant concepts (tags) of a photo.

III. PROPOSED SYSTEM

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. A policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users‟ social features. Anna CinziaSquicciarini developed an Adaptive Privacy Policy Prediction (A3P)system, a free privacy settings system by automatically generating personalized policies. The A3P system handles user uploaded images based on the persons personal characteristics and images content and metadata. The A3P system consists of two components: A3P Core and A3PSocial. 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 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. Users who have several family members among their social contacts may share with them pictures related to family events. In light of these considerations, it is important to find the balancing point between the impact of social environment and users‟ individual characteristics in order to predict the policies that match each individual's needs. Moreover, individuals may change their overall attitude toward privacy as time passes. In order to develop a personalized policy recommendation system, such changes on privacy opinions should be carefully considered.

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. Finally propose a new authentication scheme "Color Scheme Authentication". Instead of just words we propose a system in which authentication is done using colors and numbers. Users can give values from 1 to 8 for the given 8 colors. Users can even give same value for two different colors. This makes the authentication method risk free of shoulder attack, dictionary attack, eves dropping etc.

IV. 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, A3Pcore 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 (addition of new friends, new posts on one's profile etc). In above cases, it would be beneficial to report to the user the latest privacy practice of social communities that have similar background as the user. The A3P-social groups users into social communities with similar social context and privacy preferences, and continuously monitors the social groups. When the A3P-social is invoked, it automatically identifies the social group for the user and sends back the information about the group to the A3P-core for policy prediction. At the end, the predicted policy will be displayed to the user. If the user is fully satisfied by the predicted policy, he or she can just accept it. Otherwise, the user can choose to revise the policy. The actual policy will be stored in the policy repository of the system for the policy prediction of future uploads.

V. IDENTIFYING SOCIAL GROUPS

The policy recommendation process based on the social groups that a user U uploaded a new image and the A3P-core invoked the A3P-social for policy recommendation. The A3P-social will find the social group which is most similar to user U and then choose the representative user in the social group along with his images to be sent to the A3P-Core policy prediction module to generate the recommended policy for user U. Given that the number of users in social network may be huge and that users may join a large number of social groups, it would be very time consuming to compare the new user's social context attributes against the frequent pattern of each social group. In order to speed up the group identification process and ensure reasonable response time, we leverage the inverted file structure to organize the social group information. The inverted file maps keywords (values of social context attribute) occurring in the frequent patterns to the social groups that contain the keywords. Specifically, in first sort the keywords (except the social connection) in the frequent patterns in an alphabetical order. Each keyword is associated with a link list which stores social group ID and pointers to the detailed information of the social group.

VI. FEW RECENTLY IMPLEMENTED TECHNIQUES FOR PRIVACY OF UPLOADED IMAGES

A .An improved Privacy of User Data and Images on Content Sharing Sites using BIC:

Social Network is an emerging e-service for content sharing sites (CSS). It is emerging service which provides a reliable communication. Though this communication is a new attack ground for data hackers; they can easily misuse the data through these media. Some users over CSS affect users privacy on their personal content, where some users keep on sending unwanted comments and messages by taking advantage of the user's inherent trust in their relationship network. By this, privacy of the user's data may be lost. For this issue, this paper handles the most prevalent issues and threats targeting different CSS recently. This proposes a privacy policy prediction and access restrictions along with blocking scheme for social sites using data mining techniques. To perform this, the system utilizes APP (Access Policy Prediction) and Access control mechanism by applying BIC algorithm (Bayesian Information Criterion).

B. Privacy-Aware Image Classification:

Training neutral networks is a computationally intensive task that is best suited for massively parallel machines like GPUs or server farms, and as such, users realistically would have to give their data to the cloud for building the classifier. When giving this data away to be processed, it is at risk of being taken by non-intended parties. In this work, we propose modifying the data being sent; in this case images, such that if it were intercepted, it would be difficult to re-construct the original image. We propose multiple methods for achieving this privacy strategy and show the tradeoffs encountered in these scenarios.

C. Recommending Flicker groups with social topic model:

The explosion of multimedia content in social media networks raises a great demand to develop tools in order to facilitate producing, sharing and viewing media content. Particularly, Flickr groups, self-organized communities with declared, common interests, are able to help users to conveniently participate in social media network. In this paper, we address the problem of automatically recommending groups to users. We propose to simultaneously exploit media contents and link structures between users and groups. To this end, we present a probabilistic latent topic model to model them in an integrated framework, expecting to jointly discover the latent interests for users and groups and simultaneously learn the recommendation function. We demonstrate the proposed approach on the dataset crawled from Flickr.com

D. The PViz Comprehension Tool for Social Network Privacy Settings:

User's mental models of privacy and visibility in social networks often involve natural subgroups, or communities, within their local networks of friends. Such groupings are not always explicit, and existing policy comprehension tools, such as Facebook's Audience View, which allows the user to view her profile as it appears to each of her friends, are not naturally aligned with this mental model. In this paper, we introduce PViz, an interface and system which corresponds more directly with the way user's model groups and privacy policies applied to their networks. PViz allows the user to understand the visibility of her profile according to natural sub-groupings of friends, and at different levels of granularity. We conducted an extensive user study comparing PViz to current privacy comprehension tools (Facebook's Audience View and Custom Settings page). Despite requiring users to adapt to new ways of exploring.their social spaces, our study revealed that PViz was comparable to Audience View for simple tasks, and provided a significant improvement for more complex, group based tasks.

E. Contextual Dynamics of Group-Based Sharing Decisions:

In this paper we investigate how decisions made while using a granular access control mechanism for sharing photographs are influenced by contextual factors and properties relating to the identities of contacts. We develop analytical models using logistic regression to understand relationships between variables that affect sharing decisions. We also investigate how predefined, static groups for privacy control cope with the challenge of sharing large amounts of content associated with numerous different contexts, and whether they need to be adjusted to suit particular contexts.

F. Analyzing Facebook Privacy Settings: User Expectations vs. Reality:

The sharing of personal data has emerged as a popular activity over online social networking sites like Facebook. As a result, the issue of online social network privacy has received significant attention in both, research literature and the main stream media. Our overarching goal is to improve defaults and provide better tools form an aging privacy, but we are limited by the fact that the full extent of the privacy problem remains unknown. There is little quantification of the incidence of incorrect privacy settings or the difficulty users face when managing their privacy.

G. Tag, You Can See It! Using Tags for Access Control in Photo Sharing:

Users often have rich and complex photo-sharing preferences. But properly configuring access control can be difficult and time consuming. In an 18-participant laboratory study, we explore whether the keywords and captions with which users tag their photos can be used to help users more intuitively create and maintain access-control policies. We find that (a) tags created for organizational purposes can be repurposed to create efficient and reasonably accurate access control rules; (b) users tagging with access control in mind develop coherent strategies that lead to significantly more accurate rules than those associated with organizational tags alone; and (c) participants can understand and actively engage with the concept of tag-based access control.

H. Using Web Co-occurrence Statistics for Improving Image Categorization:

Object recognition and localization are important tasks in computer vision. The focus of this work is the incorporation of contextual information in order to improve object recognition and localization. For instance, it is natural to expect not to see an elephant to appear in the middle of an ocean. We consider a simple approach to encapsulate such common sense knowledge using co-occurrence statistics from web documents. By merely counting the number of times nouns (such as elephants, sharks, oceans, etc.) co-occur in web documents, we obtain a good estimate of expected cooccurrences in visual data. We then cast the problem of combining textual co-occurrence statistics with the predictions of image-based classifiers as an optimization problem. The resulting optimization problem serves as a surrogate for our inference procedure. Albeit the simplicity of the resulting optimization problem, it is effective in improving both recognition and localization accuracy. Concretely, we observe significant improvements in recognition and localization rates for both Image Net Detection 2012 and Sun 2012 datasets.

Personalized Portraits Ranking:

Portraits, also known as images of people, constitute an important part of consumer photos. Existing methods manage portraits based on either explicit objectives, e.g., a specified person or event, or aesthetics, i.e., the aesthetic quality of portraits. This paper presents a novel system for personalized portraits ranking. First, four kinds of personalized features, i.e., composition, clothing style, affection and social relationship are proposed to quantify user’s intent. Then, example-based and sketch-based user interfaces (UI) are developed, which are capable of capturing user’s personal intent hardly described by queries or aesthetics. Finally, portrait ranking is implemented by combing these features together with the developed user interfaces. Experimental results show that the system performs well in providing personalized preferences and the proposed features are effective for portrait ranking. From the user study, our system gets promising results.

VII. IMPLEMENTATION

This paper 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 consists of two main components: A3P-core and A3P-social. 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. 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.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.

A.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. In the above definition, Subject(S) can be user's identities, relations such as family, friend, coworkers, 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. 2015)]. allowed.

B. 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 behavior 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.

C. A3P Core

The A3P Core consists 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 generalized. 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.

VIII. 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.

IX. REFERENCES

[1]. H. Lipford, A. Besmer, and J. Watson, “Understanding privacy settings in facebook with an audience view,” in Proc. Conf. Usability, Psychol., Security, 2008.

[2]. N. Zheng, Q. Li, S. Liao, and L. Zhang, “Which photo groups should I choose? A comparative study of recommendation algorithms in flickr,” J. Inform. Sci., vol. 36, pp. 733–750, Dec. 2010.

[3]. J. Yu, D. Joshi, and J. Luo, “Connecting people in photo-sharing sites by photo content and user annotations,” in Proc. IEEE Int.Conf. Multimedia Expo, 2009, pp.1464–1467.

[4]. C.-H. Yeh, Y.-C. Ho, B. A. Barsky, and M. Ouhyoung, “Personalized photograph ranking and selection system,” in Proc.Int. Conf. Multimedia, 2010, pp. 211–220. [Online]. Available: http://doi.acm.org/10.1145/1873951.1873963.

[5]. K. Strater and H. Lipford, “Strategies and struggles with privacy in an online social networking community,” in Proc. Brit. Comput Soc. Conf. Human-Comput. Interact. 2008, pp.111–119.

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

[7]. 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.

[8]. A. Mazzia, K. LeFevre, and A. E.,, “The PViz comprehension tool for social network privacy settings,” in Proc. Symp. Usable Privacy Security, 2012.

[9]. M. Rabbath, P. Sandhaus, and S. Boll, “Analysing Facebook features to support event detection for photo-based facebook applications,” in Proc. 2nd ACM Int. Conf. Multimedia Retrieval, 2012, pp. 11:1–11:8.

[10]. Dan Lin, Sundareswaran. S, Wede.J, ”Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites” in Proc. IEEE Int. Volume.27, Issue.1Jan. 1 2015

AUTHOR’S PROFILE

V.SUDHARSHAN received the M.Tech degrees in Computer Science & Engineering and Information Technology from the JNTUH University, Hyderabad, in 2005 and is currently pursuing the Ph.D. degree in Computer Science & Engineering at the JNTUH—Hyd. He has a vast experience in network-related & software-development from several startup companies. His research interests include Secure Cloud Computing, content caching, cellular networks, and traffic redundancy elimination

SK.NAGASAIDULU, received the M.Tech degree in computer science and engineering from the JNTU-H in 2013. Presently Working As Assistant Professor In Khammam Insttitute Of Technology & Sciences-Khammam.

BOJJA KALPANA received her graduate degree in B.Tech. Computer Science and Engineering from JNTU-H in the year of2014.Pursuing Post graduate degree M.Tech. Computer Science and Engineering from Khammam Institute of Technology and Science Affiliated to JNTU-H in the year of 2016. She is interesting in Java.