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. 3, Issue 9, September 2015

A Survey on User-Uploaded Images Privacy Policy Prediction Using Classification and Policy Mining

Aishwarya Singh[1], Bhavesh Mandalkar[2], Sushmita Singh[3] , Prof. Yogesh Pawar[4]

B.E Student, Dept. of Computer, Dr.D.Y.Patil Institute of Engineering & Technology, Talegaon, Pune University, India[1, 2, 3]

Professor, Dept. of Computer, Dr.D.Y.Patil Institute of Engineering & Technology, Talegaon, Pune University, India[4]

ABSTRACT: Social media's become important part of our daily life. Using social media we are able to communicate with lot of people. Facebook is most popular example of social media which enable us to communicate with lot of people. In which peoples have opportunities to meet new peoples, friends and communicate with each other. Peoples or users also share images, personal information through social site so maintaining privacy is a most important task. Because of large amount of image share through social sites image privacy is a major problem. There is a need of a tool which helps users to control access to their shared content. In this paper an Adaptive Privacy Policy Prediction is used to help user for privacy setting of their image. Our goal is to provide various privacy policy approaches to improve the privacy of images or information shared in the social media site..

KEYWORDS: Social media; content sharing sites; Privacy; Meta data

I. Introduction

Nowadays sharing photos on Web is very popular. In many web sites such as in Flicker user can upload their photos and also describe them by tags. While sharing their photos on these web sites users want their privacy. Currently, In most photo sharing sites users can only specify whether a photo is private, public or visible to their friends or those who are there family member. This setting can be applied by user to particular photo or a set of particular photos. They cannot share photos with only, for example, to those people who were participated in any particular event. If users move to another sharing site then list of friends also may have to compile again. In these website tags are widely used on photos. These tags are providing rich information about photos. So, by using tags assigned to the photos a better access control mechanism can be provided. Most content sharing websites allow users to enter their privacy preferences. But users have to struggle hard to set up such privacy. Maintenance of such privacy settings are also hard [1]. This process can be error prone and tedious. In this paper, an Adaptive Privacy Policy Prediction (A3P) system is used to provide users privacy settings easily by automatically generating personalized policies. This system handles user uploaded images.

Following criteria is used to influence privacy setting of image:

- *Personal characteristics and impact of social environment:*

User's social content can provide useful information about users .These content may be their profile picture and their relationship with other users. For example, users who are interested in photography may want to share photos with other photographer.

The role of image's content and metadata

In general, images which are of similar type require similar privacy preferences, mainly when people appear in the images. For example, one may upload photos of their Childs and want that only his family member can see and comment on these photos. He may upload some others photos of flowers which he took as a hobby. For which he may set privacy preference as allowing anyone to view and comment on these photos.

Building blocks (as shown in Figure): A3P-Social and A3P-Core. In A3P core first user's image is classified based on content and metadata then privacy prediction done by analysing privacy policies of each category of images. A3P-Social is used to extend the prediction power of our system. In this a mechanism is used to generate privacy policies based on information related to user's social content and his general attitude toward privacy.A3P social is used in two cases ,first when user is new and second when system found some changes of privacy trend in social content.

System overview: Input of our A3P system is user uploaded image. When users upload an image then it first goes to A3P core. Which work is to first classify the image and then determine its policy. Mainly policy is determined based on historical data. A3P-core has to classify image and determine that A3P social net to invoke or not.A3P invoke A3P social if one of the following condition occur :-(i) To construct policy prediction user does not have enough information. (ii)If major change is detected by A3P-core in community of users, for example when new friends are added or any new posts found on one's profile. In these cases, it will report latest privacy practice to the user of social communities that have similar background as the user. The A3P-social groups user with those social communities which have same background as user. The A3P-social automatically determines the user's social group .After that it sends back group information to the A3P-core for policy prediction. After policy prediction, predicted policy will displayed to user. if user satisfy they can accept that policy otherwise he can revise the policy. The actual policy will be store in repository for future image uploads.

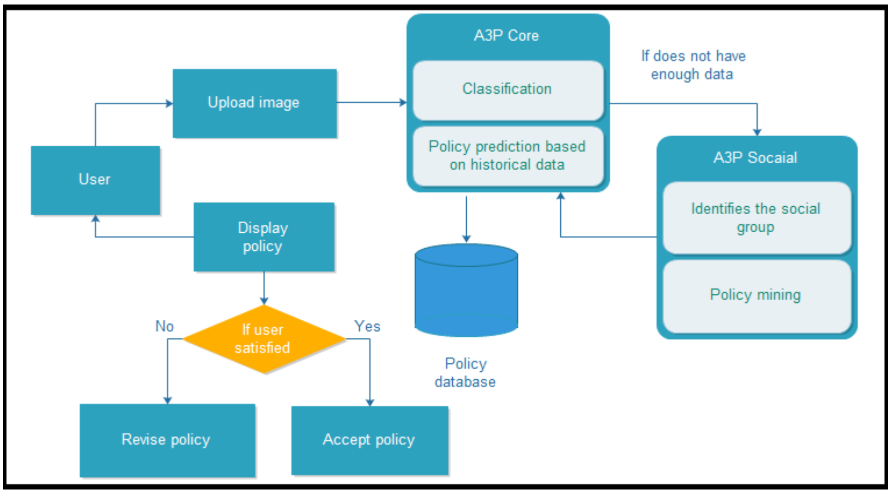

Fig. System Overview

II. LITRATURE SURVAY

2.1 Jonathan Anderson proposed Privacy Suites by which users can easily choose "suites" of privacy settings. This can be created by an expert using privacy programming. It could also be created directly through existing configuration UIs. By exporting them to the abstract format also, privacy suites can be created. By existing distribution channels privacy suite is distributed to the members of the social sites. A rich programming language is less understand ability for end users. Motivated users should be able to verify a Privacy Suite by high level language. The main goal is transparency.

2.2 Fabeah Adu-Oppong uses the concept of social circles to develop privacy setting. This privacy setting provides a web based solution to protect personal information. The Social Circles Finder technique is used to automatically generate the friend's list. This social circle of a person is analysis by this technique. It identifies intensity of relationship. This application identifies the social circles of the subject but not show them to the subject. The subject will then be asked questions about their willingness to share their personal information. Based on the answers the application finds the visual graph of users.

2.3 Kambiz Ghazinour designed a system known as Your Privacy Protector [4] .It understands the social net behaviour of their privacy settings. Recommending reasonable privacy options are also understands by this system. It uses user's personal profile, User's interests as parameters and by using this parameter the system constructs the personal profile of the user. It automatically learned profile of users and assign the privacy options. User see their current privacy settings on their social network with the help of the system, namely facebook, and the possible privacy risks is monitor and detected. It adopts the necessary privacy settings based on the risks.

2.4 Alessandra Mazzia designed PViz Comprehension Tool [5], an interface and system that more directly with privacy policies and users' model groups applied to their networks. The users understand the visibility of her profile according to constructed natural sub groupings of friends automatically and at different levels of granularity using the PViz tool. The users are able to identify and distinguish automatically-constructed groups. Users also address the sub-problem to produce group labels which will effective. PViz is better than other tools Facebook's Audience View and Custom Settings page.

2.5 In social media sites Peter F. Klemperer introduces a tag based access control of data [6] shared. Using photo management tags system creates access-control policies. With the participant's friends every photo is incorporated with access grid. A suitable preference and access information is selected by the participants. Based on the user's needs we can categories photo tags as organizational or as communicative. Several important limitations are available to our study design. First, results are limited by the participants we recruited and the photos they provided. Second limitation is access –control rules generated by machine. When tagging for access control the algorithm has no access to the context and to the meaning of tags and no insight into the policy the participant. Some rules appeared arbitrary to the participants, potentially driving these rule toward explicit policy-based tags such as "private" and "public as a result.

2.6 In sematic WebChing-man Au Yeung develop a access control system based on a protocol called decentralized authentication [6].It was based on descriptive tags and linked data of social networks. Expressive policies created by user using the access control system for their photos which is stored in one or more than one photo sharing sites. It allows users to access control rules based on open linked data provided by other parties.

2.7 Sergej Zerr develops a technique named as Privacy-Aware Image Classification and Search [8] .It automatically detect private images, and to enable privacy-oriented image search. Using this technique we can provide security policies to combines textual meta data images with variety of visual features. By selected image features like edges, faces, colour histograms we can difference between natural and man-made objects or scenes that indicate the presence or absence of particular objects (SIFT). With the help of privacy assignments obtained by a social annotation game this technique uses several classification models trained on a large scale dataset.

III. PROPOSED METHOD

3.1 Model

The aims of Adaptive Privacy Policy Prediction (A3P) system to provide users a hassle free privacy settings experience by automatically generating personalized policies.

Two main building blocks of the proposed A3P system is comprised as A3P-Social and A3P-Core. The focuses of A3P-core is to analyzing each individual user's own images and metadata,the A3P-Social provide community perspective of privacy setting recommendations for a user's potential privacy improvement. we design the interaction flows between two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice.

3.2 Image Classification

Image Classification hierarchical image classification which classifies images first based on their contents and after that refine each category into subcategories based on their metadata. If image have not metadata then it will be grouped only by content. Such as hierarchical classification gives a higher priority to image content and it minimizes the influence of missing tags . Note that Multiple categories of some images are included as till they contain the typical content features or metadata of those categories that it is possible .

DOI: 10.15680/IJIRCCE.2015. 0309025

3.3 Mining

For policy mining we approach mining hierarchical mining. Our approach leverages in policies is association rule mining techniques to discover popular patterns . The same category of the new image the policy mining is carried out because similar level of privacy protection is provided in the same category of the image. The basic idea of the hierarchical mining is to follow a natural order in which a user defines a policy. when given an image, a user first decides who can access the image , then what specific access rights (e.g., view only or download) should be given is thinks by the user, and finally refine the access conditions.First search popular subjects defined by the user corresponding to the hierarchic mining, the search of popular actions in the policies containing the popular subjects, and finally Both popular subjects and conditions which are containing by those polices that is the popular conditions .

IV. Conclusion and Future Work

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.

Acknowledgement

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure support. Finally, we would like to extend heartfelt gratitude to friends, family members.

References

[1] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.

[2]. 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.

[3] 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.

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

[5].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.

[6].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. 9–14.

[7].Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova , I Know What You Did Last Summer!:Privacy-Aware Image Classification and Search , Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval, 2012.

[8]. Anna Cinzia Squicciarini, "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites", IEEE Transactions on Knowledge and Data Engineering, vol. 27, no. 1, January 2015.

[9]. K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," in Proc. Brit. Compute.

[10]. Soc. Conf. Human-Compute. Interact, 2008, pp.111–119.

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

[12].. 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.

[13]. Mehmet Erkan Yüksel and Asım Sinan Yüksel, "An Application for Protecting Personal Information on Social Networking Websites", The Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2010.

BIOGRAPHY

Aishwarya Singh is a B.E student in the Computer Engineering Department, Dr. D. Y. Patil Institute of Engineering and Technology, Ambi, Talegaon, Pune, Savitribai Phule Pune University.

Bhavesh Mandalkar is a B.E student in the Computer Engineering Department, Dr. D. Y. Patil Institute of Engineering and Technology, Ambi, Talegaon, Pune, Savitribai Phule Pune University.

Sushmita Singh is a B.E student in the Computer Engineering Department, Dr. D. Y. Patil Institute of Engineering and Technology, Ambi, Talegaon, Pune, Savitribai Phule Pune University.

Prof. Yogesh Pawar received M-TECH Degree from JNTO University and having 7 years of teaching experience. He has published 4 international papers.

DOI: 10.15680/IJIRCCE.2015. 0309025