IJMTST | Volume: 2 | Issue: 05 | May 2016 | ISSN: 2455-3778

Predicting Privacy Policy Automatically To the User Uploaded Images on Content Sharing Sites

Rashmi T.M[1] | V. Chetan Kumar[2]

[1]PG Scholar, Department of Computer Science and Engineering, P.E.S. College of Engineering, Mandya, Karnataka, India.
[2]Assistant Professor, Department of Computer Science and Engineering, P.E.S. College of Engineering, Mandya, Karnataka, India.

ABSTRACT

Nowadays sharing of images is increasing through social networking sites but maintaining privacy is a major problem. While sharing images users knowingly or unknowingly share their personal information. Due to these incidents, there is a need of tool for setting privacy for their images. To address this need we propose an adaptive privacy policy prediction (A3P) to set privacy for their images. We are considering the metadata for predicting the privacy. Our Solution depends on image classification for image categories and predicting privacy.

KEYWORDS: *Online information services, web-based services.*

I. INTRODUCTION

Images are the main key enablers for user to connect in social networking sites. Sharing of images takes place not only for known person or group but also for social circles e.g., Google+, Face book etc. However images may expose sensitive information of user and they may lead to unwanted risks and personal information violations[2],[6].Due to persistent nature of social media , it allows others to collect information of owner of published content.[2],[5],[6]. This may lead to expose of one's personal information. Therefore, in this paper we are implementing adaptive privacy policy prediction(A3P) system which provides risk free privacy settings automatically by generating policies[1].

Existing System

- Most social networking sites allow user to enter their privacy preferences but users struggle to maintain these types of policies.
- Because user share lot of information on social media putting privacy policies for each and everything is difficult task and error-prone.

Disadvantage of Existing System

- Images may expose sensitive information of user and they may lead to unwanted risks and personal information violations
- Due to persistent nature of social media, it allows others to collect information of owner of published content.
- This may lead to expose of one's personal information.

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.

Advantages of Proposed System

- The A3P-core focuses on analyzing each individual user's own image's metadata.
- User can set policies automatically by generated policies.

II. LITERATURE SURVEY

Some studies are carried out to set policies automatically. Bonneau et al.[3] proposed the concept of 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 modifications. Similarly, Ravichandran et al.[7] studied how to predict a user's privacy preferences for location-based data based on location and time of day. More recently, Klemperer et al.[5] studied 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.

III. System Architecture

3.1 A3P Framework

Privacy policies are privacy preferences expressed by the user to protect their information from unwanted disclosure. We define the privacy policies as follows:

Definition: A privacy policy p of user u consists of the following components:

- 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 action granted by u to S on D
- Condition(C):A Boolean expression which must be satisfied in order to perform the granted actions.

3.2 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 the following blocks as shown in the figure1:

1. Metadata based image classification
2. Adaptive policy prediction
3. Look-up privacy policies
4. Database.

A3P core classifies the images based on the metadata and predict the policies depending on the metadata. The look-up privacy policy looks if the image or similar type of image already exists which can be given with the similar privacy policies. If similar type of image doesn't exist then it looks for all the policies and lets user choose the policies.

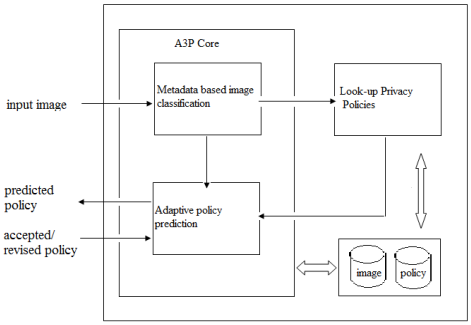

Fig 1: System architecture

3.3 A3P CORE

There are two major components in A3PCore:

1. Image classification
2. Adaptive policy prediction

3.3.1 Metadata-based image classification:

The Metadata-based image classification groups images into sub-categories. The process consists of following 3 steps:

Step 1: Extract keywords from the metadata associated with an image. The metadata considered are tags, caption and comments. Identify all the nouns, verbs and adjectives in the metadata and store them as metadata vectors.

$$\tau_{noun} = \{t_1, t_2, \ldots, t_i\}, \tau_{verb} = \{t_1, t_2, \ldots, t_j\} \text{ and } \tau_{adj} = \{t_1, t_2, \ldots, t_k\}$$

where i, j and k are the total number of nouns, verbs and adjectives respectively.

Step 2: Derive a representative hypernym (h) from each metadata vector. Retrieve the hypernym for each t_i in a metadata vector based on the Word net classification and obtain a list of hypernym

$$\eta = \{(v_1, f_1), (v_2, f_2), \ldots\}$$

where v: hypernym and f :frequency.

Step 3: Find a subcategory that an image belongs to. At the beginning, the first image forms a subcategory as itself and the representative hypernyms of the image becomes the subcategory's representative hypernyms. We compute the distance between representative hypernyms of a new incoming image and each existing subcategory [4].

3.3.2 Adaptive policy prediction

There are two major components in the Adaptive policy prediction process.

1. Policy mining
2. Policy prediction

Policy mining is a process of mining policies for similar categorized images and policy prediction process for predicting the policy for user uploaded images.

Policy mining: Privacy policies are privacy preferences expressed by the user to protect their information from unwanted disclosure. Policy mining process deals with mining of policies by applying various association rules and steps. This hierarchical approach considers subject, action and conditions. It includes following steps:

Step1: apply association rule mining on subject component of the policies of the new image. Then

select the best rule by considering the two measures like support and confidence.
Step 2 : similar to the first step apply association rule mining on action component . Then select the best rule.
Step 3: mine the condition component in each policy set. The best rules are selected which gives us a set of attributes which often appear in policies.

Policy prediction: the policy mining process may give us many number of policies, but our system needs to show the best one to the user thus, this approach is to choose the best policy for the user by obtaining the strictness level. The strictness level describes how strict a policy is. The strictness can be discovered by two metrics: major level and coverage rate. The major level is determined with the help of combinations of subject and action in policy and coverage rate is determined using the condition component statement.

IV. Conclusion

We have proposed an Adaptive privacy policy prediction (A3P) system to automate the privacy policy settings for user uploaded images. And it provides hassle free policies for user information on social networking site.

References

[1] Anna cinziz squicciarini, member,IEEE, Dan Lin,Smith 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] 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.

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

[4] L. Geng and H. J. Hamilton, "Interestingness measures for data mining: A survey," ACM Comput. Surv., vol. 38, no. 3, p. 9, 2006.

[5] P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer, L. F. Cranor, N. Gupta, and M. Reiter, "Tag, you can see it!: Using tags for access control in photo sharing," in Proc. ACM Annu. Conf. Human Factors Comput. Syst., 2012, pp. 377–386.

[6] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in Proc. ACMSIGCOMMConf. Internet Meas. Conf., 2011, pp. 61–70.

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

[8] R. A. Wagner and M. J. Fischer, "The string-to-string correction problem," J. ACM, vol. 21, no. 1, pp. 168–173, 1974.