A A3P FRAMEWORK TO PROTECT USER UPLOADED DATA IN CLOUD

K.P. RAJARAJESWARI
Student, M.Tech.,(CSE)
Dept. of CSE
kpraji93@gmail.com

N. MUNI SANKAR
Asst. professor
Dept. of CSE
ms.nagugari@gmail.com

V. JANARDHAN BABU
Professor
Dept. of CSE
ungarala66@gmail.com

ABSTRACT

With the increasing volume of images share through social sites by users, maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. In light of theseincidents, 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.Social network users expect the social networks that they use to preserve their privacy. Traditionally, privacy breaches have been understood as malfunctioning of a given system. However, in online social networks, privacy breaches are not necessarily a malfunctioning of a system but a byproduct of its workings. The users are allowed to create and share content about themselves and others. When multiple entities start distributing content without a control, information can reach unintended individuals and inference can reveal more information about the user.

Our aim is to identify when the privacy of an individual will be breached based on a content that is shared in the online social network. The content that might be shared by the users or by others, the content may vary, including a picture, a text message, a check-in information or even a declaration of personal information. Whenever such content is shared, it is meant to be seen by certain individuals; sometimes, a set of friends or sometimes, the entire social network. Whenever this content reveals information to an unintended audience, the user's privacy is breached. It is important that if a user's privacy will be breached, then either the system takes an appropriate action to avoid this or if it is unavoidable at least let the user know so that she can address the violation. In current online social networks, users are expected to monitor how their content circulates in the system and manually find out if their privacy has been breached.

To understand and study privacy violations in online social networks, we need a meta-model to describe them. A meta-model provides a language to describe models for various social networks.Social context of users, such as their profile information and relationships with others may provide useful information regarding users' privacy preferences. Users may have drastically different opinions even on the same type of images.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 personalised policy recommendation system, such changes on privacy opinions should be carefully considered.

Corresponding to the aforementioned two criteria, the proposed A3P system is comprised of two main building blocks (as shown in below figure): 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 interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice.

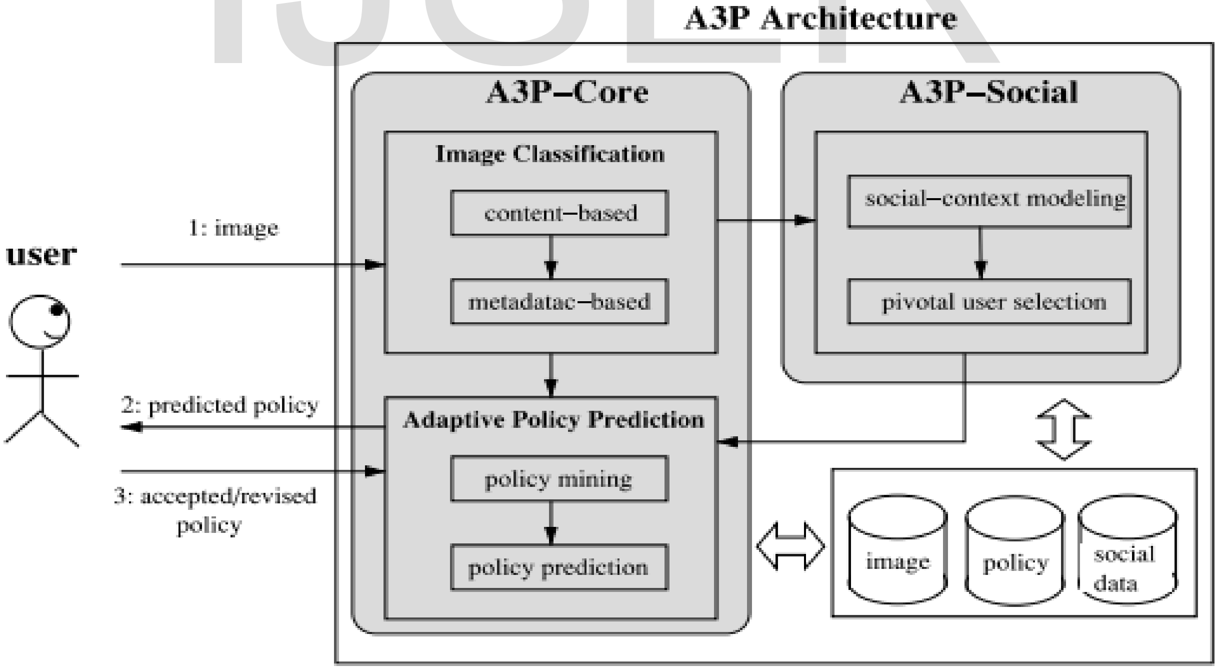

Figure: System Overview

Tags and other metadata are indicative of the social context of the image, including where it was taken and why and also provide a synthetic description of images, complementing the information obtained from visual content analysis. 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 interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice. The A3P system consists of two main components: A3P-core and A3P-social. 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 (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.

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.

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.

Content-Based Classification

Our approach to content-based classification is based on an efficient and yet accurate image similarity approach. Specifically, our classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. For each image, the wavelet transform encodes frequency and spatial information related to image color, size, invariant transform, shape, texture, symmetry, etc. Then, a small number of coefficients are selected to form the signature of the image. The content similarity among images is then determined by the distance among their image signatures groups images into subcategories under aforementioned baseline categories.

Adaptive Policy Prediction

The policy prediction algorithm provides a predicted policy of a newly uploaded image to the user for his/her reference. More importantly, the predicted policy will reflect the possible changes of a user’s privacy concerns. The prediction process consists of three main phases:

(i) Policy normalization;

(ii) Policy mining; and

(iii) Policy prediction.

The policy normalization is a simple decomposition process to convert a user policy into a set of atomic rules in which the data (D) component is a single-element set. 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 The policy mining phase may generate several candidate policies while the goal of our system is to return the most promising one to the user.

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.

Modeling Social Context

We observe that users with similar background tend to have similar privacy concerns, as seen in previous research studies and also confirmed by our collected data. This observation inspires us to develop a social context modeling algorithm that can capture the common social elements of users and identify communities formed by the users with similar privacy concerns. The identified communities who have a rich set of images can then serve as the base of subsequent policy recommendation. The social context modeling algorithm consists of two major steps.

The first step is to identify and formalize potentially important factors that may be informative of one's privacy settings.

The second step is to group users based on the identified factors. The policy mining phase may generate several candidate policies while the goal of our system is to return the most promising one to the user.

Thus, we present an approach to choose the best candidate policy that follows the user's privacy tendency. To model the user's privacy tendency, we define a notion of strictness level. The strictness level is a quantitative metric that describes how "strict" a policy is.

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. In this, we introduced a meta-model to define online social networks as agent-based social networks to formalize privacy requirements of users and their violations. In order to understand privacy violations that happen in real online social networks, we have conducted a survey with Facebook users and categorized the violations in terms of their causation.

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] M. Mondal, P. Druschel, K. P. Gummadi, and A. Mislove, “Beyond Access Control: Managing Online Privacy via Exposure,” in Proceeding of the Workshop on Useable Security (USEC), February 2014.

[7] R. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, “Open challenges in relationship-based privacy mechanisms for social network services,” International Journal of Human-

Computer Interaction, vol. 31, no. 5, pp. 350–370, 2015.

[8] F. Baader, D. Calvanese, D. L. McGuinness, D. Nardi, and P. F. PatelSchneider, Eds., The Description Logic Handbook: Theory, Implementation, and Applications. New York: Cambridge University Press, 2003.

[9] M. P. Singh, “An ontology for commitments in multiagent systems,” Artificial Intelligence and Law, vol. 7, no. 1, pp. 97–113, 1999.

[10] D. J. Solove, Understanding Privacy. Harvard University Press, 2008.