International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 5643-5647

A Comprehensive privacy policy for User Uploaded images on content sharing Networks

Dr. I Surya Prabha[1], Dr Mohammed Ali Hussain[2], Dr. P.Gayathri[3] and K.Poorna Surya Teja[4]

[1]*Associate Professor, Department of IT, Institute of Aeronautical Engineering, Dundigal, Hyderabad, India.*

Orcid: 0000-0002-9703-4340

[2]*Professor, Department of ECM, K L University, Vijayawada, India.*

[3]*Associate Professor, Department of IT, GRIET, Bachupally, Hyderabad, India.*

Orcid id:0000-0001-5384-4547

[4]*Assistant Professor, Department of IT, Sreenidhi Institute of Science & Technology, Hyderabad, India.*

Abstract

With the increasing volume of the user picture sharing through social sites, know a days keeping security has turned into a network issue, as shown by a current rush of advertised occurrences where clients unintentionally shared individual data. In light of these occurrences, the need of devices to enable user to control access to their mutual substance is clear. Toward tending to this need, we propose an Adaptive Privacy Policy Prediction (A3P) framework to enable user to create security settings for their pictures. We analyze the part of social setting, image substance, and metadata as conceivable pointers of user protection inclinations. We propose a two-level system which as indicated by the user accessible history on the site, decides the best accessible protection approach for the client's pictures being transferred. Our answer depends on a picture arrangement structure for picture classes which might be related with comparable approaches, what's more, on a strategy forecast calculation to consequently produce an approach for each recently transferred picture, additionally as per user social highlights. After some time, the created arrangements will take after the development of user protection mentality. We give the consequences of our broad assessment more than 5,000 approaches, which show the adequacy of our framework, with forecast exactnesses more than 90 percent.

Keywords: security, framework, unintentionally,picture

INTRODUCATION

Now–a-days the term connectivity has a lot of meanings because of the growth of the social groups and due to a lot of change in technological advances and the thinking of the social users. IMAGES are now one of the easier and simpler way for users' connectivity. Sharing of images becomes so popular as it creates a social status to the users. Sharing takes place among both previously established and associated groups of known people or social circles (e.g., Google+, Flickr or Picasa), and also increasingly with people outside the social circles, this helps for the purpose of social discovery-this thing help them to identify new friends and followers and also learn about peers interests and social surroundings. However, some rational informational content rich images may reveal some personal and sensitive information. For suppose take a click of the students celebrating a 2012 graduation ceremony and let it be shared within some social groups such as Google+ circle or Flickr group, but it may unnecessarily reveal the info of students, family members and friends. This type of sharing within online may lead to many problems such as revealing the private information and may lead to unwanted disclosure and privacy violations [2], [10].Further it also causes many problems because the persistent nature of online media makes it possible for all the worldwide users to collect rich aggregated information about the owner of the published content and the subjects in the published content [2], [8], [10]. This leads to unexpected exposure of one's social environment and lead to abuse of one's personal information. Till then, one's personal information of one person or user becomes social.

There are a lot of content sharing websites that we are using now- a -day and most of the content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have encountered and shown that users struggles and finding problem to set up and maintain such privacy settings [1], [6], [9], [13]. The main reasons behind this is One of the main reasons provided is that given the amount of shared information in this process can be

dull and too long and can cause some multiple errors. Therefore, most of the content sharing websites have acknowledged the need of policy recommendation systems which can help users to easily and properly configure their own privacy settings [9], [11], [12]. However, the proposals that we are using now for automating privacy settings appear to be lacking the quantity and insufficient to address the unique privacy needs of images [2], [3], [15], due to the amount of information unknowingly and indirectly carried within images, and their relationship with the online environment wherein they are exposed. In this paper, we discussed and proposed an Adaptive Privacy Policy Prediction (A3P) system which helps and supplying the users with a hassle free and irritating free and inconvenience free environmental privacy settings experience by automatically generating personalized policies. If any user shared anything, the profile information of that user such as social contexts i.e relationships with others, their martial status etc becomes open.

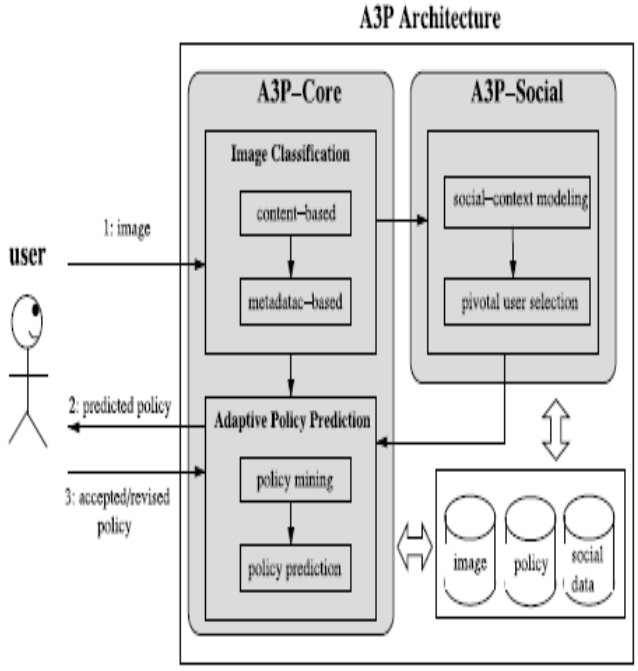

Figure: A3P Architecture

When it comes to impact of social environment on users life style by sharing such protective personal information can cause may hurdles in many ways in one's own private life. If any user shared anything, the profile information of that user such as social contexts i.e relationships with others, their martial status etc becomes open.For example, if an user is interested in photography and may like to share their photos with other amateur photographers. Sometimes users who have several family members among their social contacts may share with them pictures related to family events. However, by using same policies across all users or across users with similar qualities and interests may be too simplistic and not satisfy individual preferences. Users may have totally and extremely different opinions even on the same type of images. As a case in point, a privacy adverse person may be willing to share all his personal images, while a more conservative person may just want to share personal images

LITERATURE SURVEY

The work which is related to privacy settings configuration in social media sites, endorsement systems, and protected of online images.

Privacy Settings Configuration

Security sites which are prescribe to user's security site that expert or other trusted companions have effectively set. so that typical users can either specifically pick a setting or as it were need to do minor changes in user settings. Similarly, Danez [5] etal proposed a machine-learning -based to automatically extend the privacy settings from the social set which the information created in parallel to work.

Adu-Oppong [7] etal here simultaneously creating "social media groups" which consists from the friends list.

Ravichandran et al. [12] studied how to protect a user's privacy preferences for location-based data based on location and time of day. Fang et al. proposed privacy adept to help users grant privileges to their friends. The adept 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 reactive led assign privacy labels to the unlabeled friends. More recently, Klemperer[12] etal. studied whether the keywords and captions with which users ping their photos can be used to help users more instinctive create and maintain access-control policies. Their findings are inline with our approach: pings created for organizational purposes can be re-purposed to help create reasonably accurate access-control rules.

The preceding approaches focus on deriving policy settings for only distinct, so they mainly consideration on social context such as one friend list. While absorbing, they may not be sufficient to address challenges brought by image files for which privacy may vary considerably not just because of social context but also due to the actual image content. The images, authors in which he presented an expressive language for images uploaded in social sites. The work which is proposed to do not deal with policy expressiveness, but really it common polices specification for our predictive algorithm.

In addition, it contains a huge work on image content analysis, for categorization and clarification, retrieval and photo ranking also in the context of online photo sharing sites, such as Flickr. Of these works, Zerr's work is probably the closest

to ours. Zerr explores privacy-aware image classification using a mixed set of features, both content and meta-data. This is however a binary classification (private versus public), so the categorization task is very different than ours. Also, the authors do not see the issue of cold-start problem.

A3P FRAMEWORK

Preliminary Notions

Users can express their privacy desire about their content report preferences with their socially connected users via privacy policies. We define privacy policies according to

Definition 1. Our policies are exceptional by popular content sharing sites (i.e., Facebook, Picasa, Flickr), although the actual implementation depends on the specific content-management site structure and implementation.

Definition 1. A privacy policy P of user u consists of the following components:

- Subject (S): A set of users socially connected to 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 definition, users in S can be represented by their identities, roles (e.g., family, friend, co-workers), organizations (e.g., non-profit organization, profit organization). D will be the set of images in the user's profile. Each image has a unique ID along with some associated metadata like tags "vacation", "birthday". Images can be further grouped into albums. As for A, we consider four common types of actions:{view, comment, tag, download}.

Last, the condition component C specifies when the granted action is effective. C is a Boolean expression on the grantees' attributes like time, location, and age. For better understanding, an example policy is given below.

Example 1. Alice would like to allow her friends and coworkers to comment and tag images in the album named "vacation album" and the image named "spring.jpg" before year 2012. Her privacy preferences can be expressed by the following policy:

P= {friend, coworker}, {vacation_album, spring.jpg}, {comment, tag}, (date< 2012)_.

SYSTEM OVERVIEW

The A3P system consists of two main components: A3P-core and A3P-social. It follows.

When a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and regulate whether there is a need to invoke the A3P-social. In all most cases, the A3P-core predicts policies for the users directly based on their history based behavior. It explains two cases is verified true, A3P-core will invoke A3Psocial:

(i) The user cannot have enough data for the type of the uploaded image to conduct policy forecast.

(ii) The A3P-core detects the recent major changes among the user's community about their privacy operations 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 operations of social communities that have similar background as the user. The A3P-social groups users into social group with similar social context and privacy predications, and on-going monitors the social groups. When the A3P-social is invoked, it identifies the social group for the user and sends back the data about the group to the A3P-core for policy prediction. At the end, the predicted policy will be show 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 amend (revise) the policy. The original policy will be stored in the policy repository of the system for the policy divination of future uploads.

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 predications of each category of images are analyzed for the policy prediction. Adopting a two-stage approach is more suitable for policy advise 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 propose 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 successive policy advise. As for the one-stage mining approach, it would not be able to

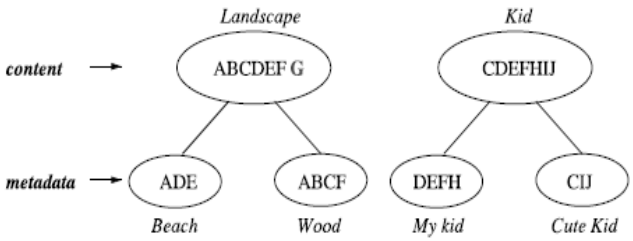

Figure: Two-level image classification

locate the right location of the new image because its classification criteria needs both image features and policies whereas the policies of the new image are not available. 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 related with privacy preferences. Here, we tend to plan a hierarchical image classification which classifies images first support based on their contents and then refine each category into subcategories based on their metadata. Images cannot have metadata will be grouped only by content. Such a hierarchical classification gives a better higher priority images and reduces 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.

Moreover, the above Fig shows an example of image classification for 10 images named as A, B, C, D, E, F, G, H, I, J, respectively. 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 sub division under each them 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".

Metadata-Based Classification

The metadata-based classification groups images into subcategories under same baseline categories. In this process we consists three main steps.

The first step is to extract keywords from the metadata associated with an image. The metadata considered in our work are tags, captions, and comments. We identify all the nouns, verbs and adjectives in the metadata and store them as metadata vectors $T_{noun}=\{t_1,t_2,\ldots t_i\}$, $T_{verb}=\{t_1,t_2,\ldots t_i\}$ and

$T_{adj}=\{t_1,t_2,\ldots t_t\}$.where i, j and k are the total number of nouns, verbs and adjectives respectively. The second step is to derive a representative hypernym (denoted as h) from each metadata vector. We first retrieve the hypernym for each t_i in a metadata vector based on the Wordnet classification and obtain a list of hypernym.$n=\{(v_1,f_1),(v_2,f_2),\ldots\ldots\}$.where v denotes hypernym and f denotes its frequency. For example, consider a metadata vector r={f"cousin","first steps", "baby boy"}. We find that "cousin" and "baby boy" have the same hypernym "kid", and "first steps" has a hypernym "initiative". Correspondingly, we obtain the hypernym list n= {(kid, 2), (initiative, 1)}. In this list, we select the hypernym with the highest frequency to be the representative hypernym, e.g., "kid". In case that there are more than one hypernyms with the same frequency, we consider the hypernym closest to the most relevant baseline class to be the representative hypernym. For example, if we have a hypernym list n ={(kid, 2), (cousin, 2), (initiative, 1)}, we will select "kid" to be the representative hypernym since it is closest to the baseline class "kids". The third step is to find a subcategory that an image belongs to. This is an incremental procedure. At the beginning, the first image forms a subcategory as itself and them representative hypernyms of the image becomes the subcategory's representative hypernyms. Then, we compute the distance between representative hypernyms of a new incoming image and each existing subcategory. Given an image, let h_n, h_a and h_v denote its representative hypernyms in the metadata vectors corresponding to nouns, adjectives

and verbs, respectively. For a subcategory c, Let h_n^c ,h_a^c, h_v^c denotes its representative hynpernyms of nouns, adjectives and verbs, respectively. The distance between the image and the subcategory is computed as a weighted sum of the edit distance between corresponding pair of representative hypernyms as shown in Equation (1), where w denotes the weight and D denotes the edit distance,

$$Dist_m=w_n.D(h_n,h_n^c)+w_a.D(h_a,h_a^c)+ w_v.D(h_v,h_v^c)\ldots\ldots\ldots\ldots\ldots (1)$$

. Note that $w_n + w_a + w_v = 1$, and $w_n > w_a > w_v$. In Equation (1), we give the highest weight to the hypernyms of the nouns because nouns are closest to the baseline classes. We consider the hypenyms of the adjectives as secondly important as the adjectives can help refine the baseline criteria. Finally, we consider the hypernymms of the verbs. By default, w_n=0:5, w_a = 0:3 and w_v = 0:2. Next we check if the closest subcategory has the distance value smaller than a threshold. If so, the new image will be included in to the subcategory and we update the representative hypernyms of the subcategory by keeping the hypernyms with the highest frequency.

CONCLUSION

We have proposed an Adaptive Privacy Policy Prediction (A3P) system that able to work for users automate the privacy policy settings approach for their uploaded images. The A3P system provides a inclusive framework to infer privacy preferences based on the information available for a given user. We additionally successfully handled the issue of cold-start, utilizing social context data. Our experimental study that demonstrates that our A3P is a practical tool that offers significant improvements over current approaches to privacy.

REFERENCES

[1] Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the face book," in Proc. 6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006, pp. 36–58.

[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] 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.

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

[5] 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.

[6] L. Church, J. Anderson, J. Bonneau, and F. Stajano, "Privacy stories: Confidence on privacy behaviors through end user programming," in Proc. 5th Symp. Usable Privacy Security, 2009.

[7] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, "Social circles: sTackling privacy in social networks," in Proc. Symp. Usable Privacy Security, 2008.

[8] 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.

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

[10] 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.

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

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

[13] 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.

[14] 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. Available: http://doi.acm.org/10.1145/1873951.1873963.

[15] 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.