Implementation of Privacy Policy Specification System for User Uploaded Images over Popular Content Sharing Sites

Miss. Minal R Hirulkar
Student of M.E, Department of Computer Science and Engineering, H.V.P.M.'s C.O.E.T.
Amravati, India
minalhirulkar@gmail.com

Prof. Vinod Gangwani
Assistant Professor, Department of Information Technology, HVPM's College of Engineering & Technology,
Amravati, India
vinod.gangwani@gmail.com

***Abstract*—**The regular use of social networking websites and application encompasses the collection and retention of personal and very often sensitive information about users. This information needs to remain private and each social network owns a privacy policy that describes in-depth how user's information is managed and published. As there is increasing use of images for sharing through social sites, maintaining privacy has become a major problem. In light of these incidents, the need of tools to aid users control access to their shared content is necessary. This problem can be proposed by using an Privacy Policy Specification system to help users compose privacy settings for their shared images. Toward addressing this need, we propose Privacy Policy Specification system to help users to specify privacy settings for their images. Privacy Policy Specification System configure a policy for a group and apply appropriate policies (comment, share, expiry, download) on image for sharing in the group.

Keywords — *Policy Mining, Image Security, Social Networking.*

*****

I. INTRODUCTION

Social media's become one of the most crucial part of our daily life as it enables us to communicate with a lot of people. With the extensive use of digital cameras and the increase of content sharing websites (eg. Flickr, Picasa, etc.) people can now easily publish their photos or videos online and share them with family, friends, coworkers, etc. While extremely convenient, this new level of pervasiveness introduces acute privacy issues. semantically rich images may reveal content sensitive information. Consider a photo of a students 2011 graduation ceremony, for example. It could be shared within a Google+ circle or Flickr group, but may unnecessarily expose the students BApos family members and other friends.

Revealing personal content on social networking services can expose sensitive information about users. These services typically allow users to create connections to 'friends' such that this content can be shared amongst them and restricted from the wider public. However, these connections rarely distinguish between different types of relationship. Even within a network of 'friends', users may wish to manage the sharing of information and content with different people based on their differing relationships.

Tools for maintaining privacy settings in social media frequently couple control (specifying who can access what) with awareness and comprehension (understanding who can access what, given the existing configuration). However, existing tools do not necessarily account for the types of "queries" users would like to make to reconcile their mental models of the system state (or desired state) with the policy defaults of the system, the limitations of the system's privacy management features, and individually-enacted settings.

Sharing images within online content sharing sites, therefore, may quickly lead to unwanted revelation and privacy violations. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information. Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and preserve such privacy settings [1], [2], [3]. 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 specification systems which can help users to easily and properly configure privacy settings [4], [3], [5], [6]. However, existing proposals for automating privacy settings appear to be insufficient 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 existing methodology, Adaptive Privacy Policy Prediction (A3P) system helps users compose privacy settings for their images. They examine the role of social context, image content, and metadata as possible indicators of user's privacy preferences. They propose a two-level framework which according to the user's available history on the site determines the best available privacy policy for the user's images being uploaded. Their solution relies on an image classification framework for image categories which may be associated w3ith similar policies, and a policy prediction

algorithm to automatically generate a policy for each newly uploaded image, also according to user's social features. But, after uploading images, sometimes system provides unnecessary privacy policy and it is not possible for user to update the policy.

In proposed methodology, we design a system in which we configure a policy for a group and apply appropriate policies on images for sharing in the group. We design a system in such a way that it provides the privacy policy that user actually need and it is also possible for user to update the privacy policy according to their need.

II. LITERATURE REVIEW AND RELATED WORK

Bonneau et al. [7] 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 modification. Adu-Oppong et al. [8] develop privacy settings based on a concept of "Social Circles" which consist of clusters of friends formed by partitioning users' friend lists. Ravichandran et al. [6] studied how to predict a user's privacy preferences or location-based data (i.e., share her location or not) based on location and time of day. Fang et al. [5] 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. More recently, Klemperer et al. [9] 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.

The aforementioned approaches focus on deriving policy settings for only traits, so they mainly consider social context such as one's friend list. While interesting, they may not be sufficient to address challenges brought by image files for which privacy may vary substantially not just because of social context but also due to the actual image content. As far as images, authors in [10] have presented an expressive language for images uploaded in social sites.

Social networking services present many advantages for information dissemination and interpersonal communication, but the copresence of multiple social groups from different facets of a user's life can present a significant challenge for controlling privacy and online identity. Many users experience a perceived loss of control over their personal information and content when using online social networking services [11].

Default privacy settings on services such as Facebook are often configured such that content is shared uniformly with all of a user's contacts. Achieving fine-grained control is an arduous process, yet people consider such control important for presenting multiple versions of themselves [12] or for minimizing the appearance of characteristics that are contrary to an idealized version of themselves [13]. Ackerman and Mainwaring [14] emphasize that, while valued, privacy is not the users' primary task and making it an explicit task for the user can be problematic. Designing privacy management tools that do not require significant configuration effort from the user is therefore an important and worthwhile objective. Systems that automate, recommend or assist with privacy management decisions could reduce the burden placed on users while providing satisfactory levels of control.

Gross and Aquisti study privacy settings in a large set of Facebook users, and identify privacy implications and possible risks. Lange [18] studies user behavior with respect to revealing personal information in video sharing. All of these papers point out lack of user awareness regarding exposure of aggregated contextual information arising from users' resource sharing habits.

There is a plethora of work dealing with the problem of establishing suitable access policies and mechanisms in social Web environments. Caminati and Ferrari [19], for example, propose collaborative privacy policies as well as techniques for enforcing these policies using cryptographic protocols and certificates. Felt and Evans [20] suggest to limit access to parts of the social graph and to certain user attributes. Squicciarini et al. [21] introduce privacy mechanisms in social web environments where the resources might be owned by several users. In [22], the authors discuss the problem of defining fine-grained access control policies based on tags and linked data. The user can, for instance, create a policy to specify that photos annotated with specific tags like "party" can only be accessed by the friends specified in the user's Friend of a Friend (FOAF) profile.

Vyas et al. [23] utilize social annotations (i.e. tags) to predict privacy preferences of individual users and automatically derive personalized policies for shared content. These policies are derived based on a semantic analysis of tags, similarity of users in groups, and a manually defined privacy profile of the user. Ahern et al. [24] study the effectiveness of tags as well as location information for predicting privacy settings of photos. To this end, tags are manually classified into several categories such as Person, Location, Place, Object, Event, and Activity.

Analysis of visual and textual image (meta-)data is applied to tackle a variety of problems, such as determining attractiveness [25] or quality [27] of photos, search result diversification [28], and others. Figueiredo et al. [26] analyze the quality of textual features available in Web 2.0 systems and their usefulness for classification.

III. EXISTING SYSTEM

Chen et al. [15] proposed a system named SheepDog to automatically insert photos into appropriate groups and recommend suitable tags for users on Flickr. They adopt concept detection to predict relevant concepts (tags) of a photo. Choudhury et al. [16] proposed a recommendation framework to connect image content with communities in online social media. They characterize images through three types of features: visual features, user generated text tags, and social interaction, from which they recommend the most likely groups for a given image. Similarly, Yu et al. [17] proposed an automated recommendation system for a user's images to suggest suitable photo-sharing groups.

Anna Squicciarini [29] developed an Adaptive Privacy Policy Prediction (A3P) system, a free privacy settings system by automatically generating personalized policies. The A3P handles user uploaded images based on the person's personal characteristics and images content and metadata. The A3P system consists of two 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. The disadvantage of A3P is inaccurate privacy policy generation in case of the absence of meta data information about the images. Also A3P has manual creation of meta data log data information that leads to inaccurate classification and also violation privacy.

IV. IV. PROBLEM STATEMENT

•With the increasing volume of images users share through social sites, maintaining privacy has become a major problem.

•A3P system consists of two components: A3P Core and A3P Social. The A3P core receives the image uploaded by the user, which it classifies and decides whether there is a need to call upon the A3P social. If the metadata is unavailable or if it is created manually then it may cause inaccurate classification, violation policy and even may cause inaccurate privacy policy generation.

•A3P system does not contain all the functionality and does not solve the problem of image security over social sites.

•In A3P, it is not possible for user to update privacy policy according to their need, image sharing is not secure because it automatically generates personalized policies.

•Whereas SheepDog system automatically insert photos into appropriate groups and recommend suitable tags for users on Flickr ,however there may be a chances that image is shared in a group in which we doesn't want to share.

•To solve the above problem we designed a system that includes some policies that are very crucial to share the image over social network site.

V. PROPOSED WORK

We are going to propose a Privacy Policy Specification system in which the user can easily applies policy(eg, comment, share, expiry, download) to group and when user shares image to the specific group, the privacy policy of that group will apply to that image.

The basic procedure is:

1. First user has to register and generate his/her user id and password.
2. User log in to the system if authenticated successfully.
3. User creates a group.
4. User apply policies (eg, comment, share, expiry, download) to Group.
5. When user shares image to the specific group, system retrieves group policies from database and apply to that image.
6. User updates privacy policy of group according to their need if he/she is the admin of group.
7. User can change password ,if he/she wishes to.

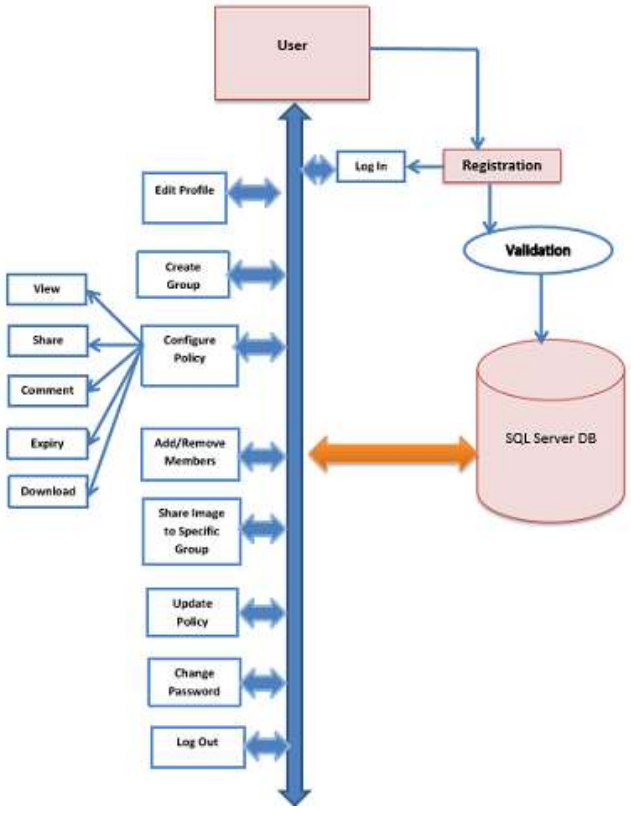

Fig 1.Architecture of Proposed System

The proposed algorithmis,

Consider,
G = Set of Groups
= {G1, G2, G3,…,Gn}
M = Set of Members in Group where, M € G
= {M1, M2, M3,…., Mn}
P = Set of Policies apply to group G where, P € G
= {P1, P2, P3,….,Pn}

Algorithm 1: For Creating Groups and Applying Policies to Group
Step 1: Start
Step 2: Add Group G1.
Step 3: Set P = {P1=View, P2= Comment, P3= Download, P4=Share, P5= Expiry}
Step 4: For each P,
If Pi = = True then Apply Pi to Group G1
else
Set Pi= False for Group G1
Step 5: End

Algorithm 2: For Sharing Images to Particular Group
Step 1: Start
Step 2: Initialize all Group G, Member M and Policies P.
Step 3: Select Image I1 to share and Group G1 from set of groups G.
Step 4: Initialize Policies P for group G1.
Step 5: For each P € G,
If Pi = = True
then Apply Pi to Image I1.
Step 6: Insert Image I1 to G and also share I1 to all Member M in the Group G1.
Step 7: End

VI. RESULT

This study involved 100 participants (70 female and 30 males) who were participated from one of the colleges in Amravati. Their average age is between 18 to 23. 80% students go through all the system and completed all the necessary steps and 20% left the system after two or three steps. The procedure of the system is, first the user has to register in the system then he/she can log in into system. After that user has to create a group and apply policies to group. Policies are view, comment, expiry, download and share. According to user requirement user can apply policies to group. User have to add members to the group and share image with the specific group. Then user checks whether image is shared or not and the policies are applied correctly or not.

In the first part, the participants were asked to indicate any social networks they were a part of (98 percent indicated Facebook and 37 percent also indicated others like Myspace). In terms of usage frequency, 95 percent of the respondents accessed social network sites at least once a week, with 76 percent of reporting that they were daily users.

We also asked participants if they have had concerns about their privacy due to shared images. Over 90 percent of the participants indicated that they had privacy concerns. Users also reported that image content is an important factor when determining privacy settings for an image with 87 percent of people agreeing or strongly agreeing with the statement “When I set privacy settings for a certain image”, and over 91 percent of users agreeing or strongly agreeing with the statement “The content of an image determines whether I upload the image to a social network site.” Surprisingly, however, many users indicated that they never changed privacy settings for group (38 percent) or changed their settings only 1 or 2 times (36 percent) since joining the system. There seems to be a clear disconnect between users privacy inclinations and their practice ofsetting privacy policies. The possible reason could be “Changing privacy settings for every image uploaded on a social site can be very time consuming”, as strong agreed or agreed by 80 percent ofusers.

In the second part, we asked users some questions, 1) “Is our system user friendly?” 78% student agreeing with the fact that the system is user friendly rest 22% says it is not user friendly. 2) “Do you understand the system or not?”, 89% students says they understand the system very well and it is quite easy to understand while 11% says they have some problem in understanding the system. 3) “Policies are understandable?” , 85% user says it is quiet easy to understand. 4) “To check whether the policies are applied correctly or not?” , 87% student says it is applied properly and 13% says it is not applied correctly.

So, our experimental study evaluates that the overall performance of our system is84.75%.and it solves the problem of“Changing privacy settings for every image uploaded on a social site is very time consuming” by applying policies to group.

VII. CONCLUSION

We have proposed Privacy Policy Specification system that helps users to configure a policy for a group and apply appropriate policies (comment, share, expiry, download) on image for sharing in the group. We also effectively tackled the issue by adding the expiry policy to the privacy policy specification system. Our experimental study proves that our system is a practical tool that offers significant improvements over current approaches to privacy.

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] 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.

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

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

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

[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 L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security,2009.

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

[9] 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.

[10] 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.

[11] Hewitt, A. and Forte, A. (2006), Crossing boundaries: Identity management and student/faculty relationships on the Facebook, Proc. CSCW06. ACM.

[12] DiMicco, J. M. and Millen, D. R. (2007). Identity management: multiple presentations of self in facebook. Proc. GROUP '07. ACM, 383-386.

[13] Goffman, E. (1959). The Presentation of Self in Everyday Life. New York: Doubleday.

[14] Ackerman, M. and Mainwaring, S. (2005). Privacy Issues in Human-Computer Interaction. In L. Cranor and S. Garfinkel (Eds.), Security and Usability: Designing Secure Systems that People Can Use, 381-400, Sebastopol, CA, O'Reilly.

[15] H.-M. Chen, M.-H. Chang, P.-C. Chang, M.-C. Tien, W. H. Hsu,and J.-LWu,"Sheepdog: Group and tag recommendation for flickr photos by automatic search-based learning," in Proc. 16th ACM Int. Conf. Multimedia, 2008, pp. 737–740.

[16] M. D. Choudhury, H. Sundaram, Y.-R. Lin, A. John, and D. D. Seligmann, "Connecting content to community in social media via image content, user tags and user communication," in Proc.IEEE Int. Conf. Multimedia Expo, 2009, pp.1238–1241.

[17] 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.

[18] P. G. Lange. Publicly private and privately public: Social networking on youtube. JCMC'08.

[19] B. Carminati and E. Ferrari. Privacy-aware collaborative access control in web-based social networks. In LCNS Springer(2008), 5094, 81-96.

[20] A. Felt and D. Evans. Privacy protection for social networking platforms. In Web 2.0 SP'08.

[21] A. Squicciarini, Mohamed, and F. Paci. Collective privacy management in social networks. In WWW'09

[22] C. M. Au Yeung, N. Gibbins, and N. Shadbolt. Providing access control to online photo albums based on tags and linked data. In SSW'09.

[23] N. Vyas, A. Squicciarini, C. Chang, and D. Yao. Towards automatic privacy management in web 2.0 with semantic analysis on annotations. In CollCom'09.

[24] S. Ahern, D. Eckles, N. Good, S. King, M. Naaman, and R. Nair. Over-exposed?:privacy patterns and considerations in online and mobile photo sharing. In CHI'07.

[25] J. San Pedro and S. Siersdorfer. Ranking and classifying attractiveness of photos in folksonomies. In WWW '09.

[26] F. Figueiredo, F. Bel´em, H. Pinto, J. Almeida, M. Gonc¸alves, D. Fernandes, E. Moura, and M. Cristo. Evidence of quality of textual features on the web 2.0. In CIKM'09.

[27] C.-H. Yeh, Y.-C. Ho, B. A. Barsky, and M. Ouhyoung. Personalized photograph ranking and selection system. In MM '10, New York,USA, 2010.

[28] R. Leuken, L. Garcia, X. Olivares, and R. Zwol. Visual diversification of image search results. In WWW'09.

[29] 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.