Policy Based Sharing And Uploading Of Images On Online Networking Sites

Miss. Shweta D. Bijwe[1], Prof. P. L. Ramteke[2]

[1] *Student of ME (CSIT) Final year, HVPM COE, Amravati, India*

[2]*Associate Professor, HOD OF Dept. of IT, HVPM COE, Amravati, India*

---***---

Abstract* - *With the increasing volume of images users share through social sites, 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 these incidents, 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. We examine the role of social context, image content, and metadata as possible indicators of users' privacy preferences. We 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. Our solution relies on an image classification framework for image categories which may be associated with similar policies, and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features. Over time, the generated policies will follow the evolution of users' privacy attitude. We provide the results of our extensive evaluation over 5,000 policies, which demonstrate the effectiveness of our system, with prediction accuracies over 90 percent.

Key Words: *Social media; content sharing sites; Privacy; Meta data, A3P System*

1. INTRODUCTION

Settled gatherings of known individuals or social circles (e. g., Google+, Flickr or Picasa), furthermore progressively with individuals outside the clients social circles, for purposes of social revelation to assist them with recognizing new associates and find out about companions hobbies and social environment. Be that as it may, semantically rich pictures may uncover content sensitive data. Consider a photograph of an under studies 2012 graduation ceremony, for instance. It could be shared inside of a Google+ circle or Flickr bunch, yet might superfluously uncover the students BA pos family members and different companions. Sharing pictures inside online substance sharing sites, therefore, may rapidly lead to undesirable exposure and protection violations,[1][2]. Further, the determined way of online media makes it workable for different clients to gather rich totaled data about the proprietor of the distributed substance and the subjects in the distributed substance.[3] The totaled data can bring about unforeseen introduction of one's social surroundings and lead to manhandle of one's close to home data. Most substance sharing sites permit clients to enter their protection inclinations. Shockingly, late studies have demonstrated that clients battle to set up and keep up such protection settings.[4][5][6][7] One of the primary reasons gave is that given the measure of shared data this procedure can be dreary and slip inclined. In this way, numerous have recognized the need of arrangement proposal frameworks which can help clients to effortlessly and appropriately design security settings [8][9][10][11] . In any case, existing proposition for robotizing security settings give off an impression of being deficient to address the exceptional protection needs of pictures because of the measure of data certainly conveyed inside of pictures[5][41], and their association with the online environment wherein they are uncovered.

2. LITERATURE SURVERY

Our work is related to some existing recommendation systems which employ machine learning techniques. Chen et al. [9] proposed a system named Sheep Dog 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. [10] 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. [6] proposed an automated recommendation system for a user's images to suggest suitable photo-sharing groups.

There is also a large body of work on the customization and personalization of tag-based information retrieval (e.g. [9]), which utilizes techniques such as association rule mining. For example, [9] proposes an interesting experimental evaluation of several collaborative filtering algorithms to recommend groups for Flickr users. These approaches have a totally different goal to our approach as they focus on sharing rather than protecting the content.

3.1.Limitations Of Existing System

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 have presented an expressive language for images uploaded in social sites. This work is complementary to ours as we do not deal with policy expressiveness, but rely on common forms policy specification for our predictive algorithm.

3. SYSTEM ARCHITECTURE

3.1. A3P Framework

Privacy Policies are privacy preferences expressed by the user about their content disclosure preferences with thier socially connected users.

We define the privacy policies as follows:

Definition: A Privacy policy P can be described for user U by

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 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 above definition, Subject(S) can be user's identities, relations such as family, friend, co-workers, etc. and organizations. Data(D) consists of all the images in the user's profile. Action(A) considers four factors: View, Comment, tags and Download. Lastly the Condition(C) specifies whether the actions are effective or not.

Example 1. Joe wants to allow her friends and family to view and comment on images in the album named "birthday album" and the image named "cake.jpg" before year 2015.The policy for her privacy preference will be P: [{friend, family}, {birthday album, cake.jpg},{view ,comment}, (date< 2015)]. allowed.

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 followings blocks:

A3P Core.

1. Metadata based Image classification.
2. Adaptive policy prediction.
3. Look-Up Privacy Policies
4. Database

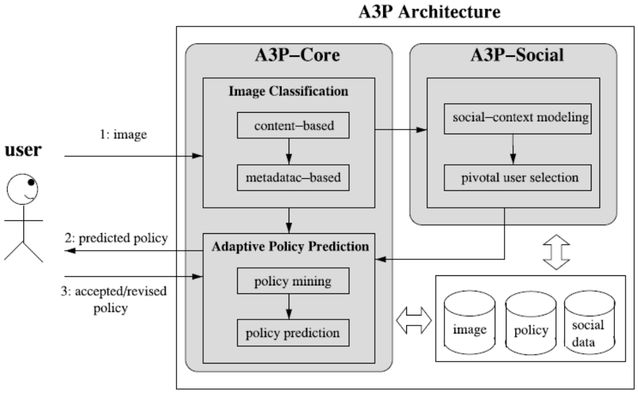


Fig.-1: A3P Architecture

A3P Core classifies the images with the help of the Metadata and also predict the policies depending upon the behaviour of the user. The Look-up Privacy Policy looks if the image or similar type of image already exists which can be given with similar privacy policies. If similar type of image doesn't exist then it looks for all the policies and lets user choose the policies.

3.3. A3P Core

The A3P Core consist of two major blocks of the framework.

1. Metadata based Image Classification
2. Content-Based Image Classification
3. Adaptive Policy Prediction

Every image of the user gets classified based on the metadata and then its privacy policies are generalized. With the help of this approach, the policy recommendation becomes easy and more accurate. Based on the Classification based on metadata the policies are applied to the right class of images. Moreover combining the image and classification and policy prediction would enhance the system's dependency.

4.3.1.Metadata Based Image Classification

The metadata-based arrangement bunches pictures into subcategories under previously stated pattern classifications. The procedure comprises of three fundamental steps. The initial step is to extricate watchwords from the metadata connected with a picture.

The metadata considered in our work are labels, subtitles, and remarks. The second step is to infer a delegate hyponym (indicated as h) from every metadata vector. The third step is to discover a subcategory that a picture has a place with. This is an incremental system. Toward the starting, the primary picture frames a subcategory as itself and the agent hyponyms of the picture turns into the subcategory's illustrative hyponyms.

4.4.2. Content-Based Image Classification

To get gatherings of pictures that might be connected with comparable protection inclinations, we propose a various levelled picture arrangement which groups pictures initially in light of their substance and afterward refine every class into subcategories in view of their metadata. Pictures that don't have metadata will be gathered just by substance. Such a various levelled characterization gives a higher need to picture content and minimizes the impact of missing labels. Note that it is conceivable that a few pictures are incorporated into numerous classes the length of they contain the run of the mill content components or metadata of those classifications.

Image selected similarity criteria include texture, symmetry, shape the image color and size. User uploads an image; it is handled as an input query image. The signature of the newly uploaded image is compared with the signatures of images in the current image database. The class of the uploaded image is then calculated as the class to which majority of the m images belong. If no predominant class is found, a new class is created for the image. Later on, if the predicted policy for this new image turns out correct, the image will be inserted into the corresponding image category in our image database.

4.3.3. Adaptive Policy Prediction

This part deals with the privacy concerns of the user by deriving the privacy policies for the images. The Adaptive Policy Prediction consists of two following sub-parts:

1. Policy Mining
2. Policy Prediction

Policy mining deals with data mining of policies for similar categorised images and Policy prediction applies prediction algorithm to predict the policies.

Policy Mining: The privacy policies are the privacy preferences expressed by the users. Policy mining deals with mining of these policies by applying different association rules and steps. It follows the order in which a user defines a policy and decides what rights must be given to the images. This hierarchical mining approach starts by looking the popular subjects and their popular actions in the policies and finally for conditions. It can be thoroughly reviewed with the help of following steps.

Step 1 of this process apply association rule mining on the subject components of the policies of the new image. With the association rule mining we select the best rules according to one of the intrestingness measure i.e., support and confidence which gives the most popular subjects in policies.

Step 2 of this process apply association rule mining on the action components. Similar to the first step we will select the best rules which will give most popular combinations of action in policies.

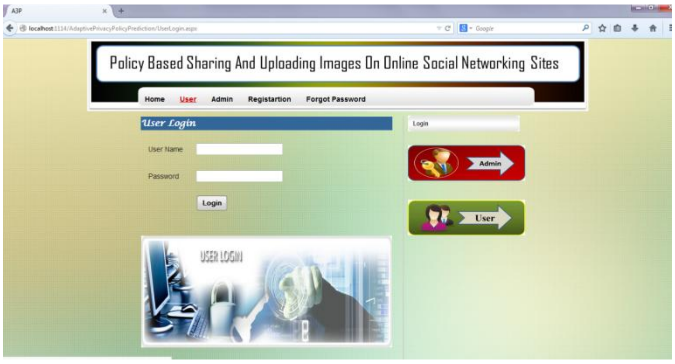
Step 3 of this process mine the condition component in each policy set. The best rules are selected which gives us a set of attributes which often appear in policies.

Policy Prediction: The policy mining phase may give us many policies but our system needs to show the best one to the user. Thus, this approach is used to choose the best policy for the user by obtaining the strictness level. The Strictness level decides how "strict" a policy is by returning an integer value. This value should be minimum to attain high strictness. The strictness can be discovered by two metrics:a major level and coverage rate. The major level is determined with the help of combinations of subject and action in a policy and coverage rate is determined using the condition statement. Different integer values are assigned according to the strictness to the combinations and if the data has multiple combinations we will select the lowest one. Coverage rate provides a fine-grained strictness level which adjusts the obtained major level. For example a user has to 5 friends and two of them are females. Hence if he specifies policy as "friends"=male, then the coverage rate can be calculated as (3/5)=0.6. Hence, the image is less restricted if the coverage rate value is high.

5. EXPERIMENTAL RESULTS

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods A3P-CORE,A3P-SOCIAL

Step 1: Login, upload image and make the privacy setting as private



Policy Based Sharing And Uploading Images On Online Social Networking Sites

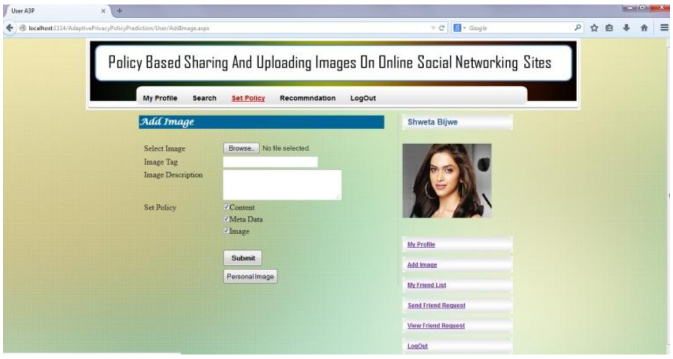
User Login

User Name

Password

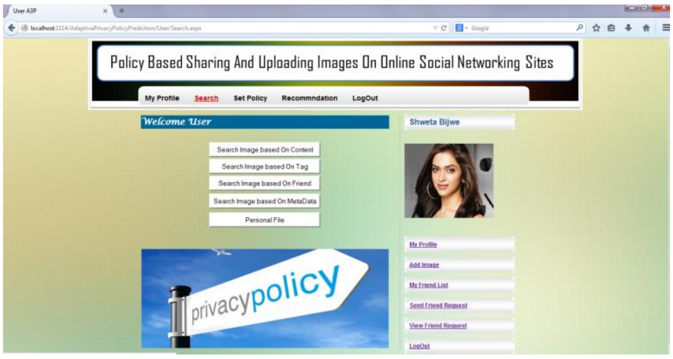
Login

Step 2: Set Policy based on Content ,Image or Meta Data on upload image and make the privacy



Select Image No file selected.
Image Tag
Image Description
Set Policy ☑ Content ☑ Meta Data ☑ Image

Step 3: Search all Images Based on Content, Tag, Metadata


User A3P
localhost:1114/AdaptivePrivacyPolicyPrediction/User/Search.aspx
Google
Policy Based Sharing And Uploading Images On Online Social Networking Sites
My Profile
Search
Set Policy
Recommndation
LogOut
Welcome User
Shweta Bijwe
Search Image based On Content
Search Image based On Tag
Search Image based On Friend
Search Image based On MetaData
Personal File
privacypolicy
My Profile
Add Image
My Friend List
Send Friend Request
View Friend Request
LogOut

6. CONCLUSION

Finally we are concluding that by providing secured privacy settings to the user uploaded images based on tags, contents and meta-data is more efficient and yields in good performance. Providing access control to the particular friends which are known and they can access the images based on permission of the uploaded user. In this we are recommending other friends also.

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on Policy Based Sharing and Uploading of Images on Online Networking Sites. I would like to take this opportunity to thank my internal guide Prof .P.L, Ramteke , Head of Information Technology Engineering Department , HVPM College of Engineering, Amravati for giving me all the help and guidance I needed. In the end our special thanks to College Management and all Staff for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

REFERENCES

[1] Anna Cinzia Squicciarini, Member, IEEE, Dan Lin, Smitha 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] J. Bonneau, J. Anderson, and L. Church, “Privacy suites: Shared privacy for social networks,” in *Proc. Symp. Usable Privacy Security*, 2009.

[3] 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

[4] 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.

[5] A. Besmer and H. Richter Lipford. Movingbeyond untagging: Photoprivacy in a tagged world. In Proceedings of the 28th international conference on Human factors in computing *systems*, pages 1563–1572. ACM, 2010.

[6] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: automatedidentity theft attacks on social networks. In Proceedings of the 18th international conference *on World wide web*, pages 551–560. ACM, 2009.

[7] 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.

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

[9] Harsh A Patel et al, Int.J.Computer Technology & Applications,Vol 6 (5),835-838 IJCTA

[10] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: automatedidentity theft attacks on social networks. In Proceedings of the 18th international conference *on World wide web*, pages 551–560. ACM, 2009.