# Enhanced Strategies with policy on Content Sharing Sites using A3P

[1]G. Kranthi, [2]Kodanda Rama Swami

[1,2]Dept. of CSE, Avanthi Institute of Engineering & Technology, Visakhapatnam, India

## Abstract

Social media's have turned out to be a standout amongst the most vital piece of our everyday life as it empowers us to speak with numerous users. Social Networking Sites like Google, Flickr and Facebook and so on are giving more chances to meet the new users and furthermore in the other various groups over the World. Users who are getting to the social-Networking administrations share their classified Information with extensive number of Friends, which may prompts Privacy Violation. On account of User's the users who are sharing the vast majority of picture information crosswise over more number of People. So there is have to enhance security as indicated by the users Satisfactory Level. Existing System named Adaptive Privacy Policy Prediction (A3P) comprises two – level Inter linkage Framework which screens the users accessible history in the sites, The A3P System helps the users by anticipating protection settings consequently for the transferred Images. The Adaptive Privacy strategy Prediction framework has extensive structure which derives protection inclinations in view of data which is accessible for a given User. Enhancing the Privacy Prediction precision over the current methodologies is the fundamental point of the Proposed System. This framework accumulates the vast majority of the users information from the substance picture sharing sites and predicts strategy forecast alongside getting to confinements alongside the blocking plans for the social networking sites by utilizing the Data Mining Techniques. To play out this, the framework uses APP (Accessing Policy Prediction) and Accessing Control Mechanism by applying the Privacy Risk Score (PRS) Algorithm.

## Keywords

Uploaded Images, Social Media, Online Information Services, Web-Based Services.

## I. Introduction

In nowadays, Images are one of the key empowering means of users connectivity. The vast majority of the circumstances picture imparting jump out at known staff like companions/families/associates and so on. Once in a while it happens with social gatherings or questions also like Picasa, Flickr, Google+ circles. Utilizing imparting to social gatherings, one tries and investigates new people and furthermore tries to find out about their likings or social angles. It has been watched that substance rich images uncover delicate data. Consider a photo of representatives greatness yearly honor work 2016.It could be imparted to companions/family finished Facebook, Flicker gathering or Google+ circle. Albeit such photo may pointlessly reveal a representative's relatives and companions. In this manner, picture sharing over social networking sites may quickly prompt improper introduction and protection infringement. Online Social sites take after the decided approach and thus makes it attainable for various users to accumulate rich abridged data about the proprietor of the common images and its substance highlights. Such removed data can release one's social attributes and prompt abuse of one's close to home points of interest. Nowadays social media sites encourage client to enter their security slants. Current systems that computerize the protection setting appear to be lacking to deal with the particular security prerequisites of images, in light of the serious inbuilt data inside images, and their relationship with the online sites wherein they are shared. This paper intricate and Adaptive Privacy Policy Recommendation framework which is intended to encourage users with effective security setting. In this paper, we propose an Adaptive Privacy Policy Prediction (A3P) framework which expects to give users an issue free protection settings encounter via naturally producing customized approaches. The A3P framework handles client transferred images, and factors in the accompanying criteria that impact one's security settings of images.

## II. Related Work

Numerous social networking sites have started constructing interfaces to help gathering, as Facebook records and Google+'s "Circles." However, existing arrangement appreciation apparatuses, for example, Facebook Audience View, are not lined up with this psychological model. PViz, an interface and framework that compares all the more specifically with how users show gatherings and protection approaches connected to their systems. PViz enables the client to comprehend the perceivability of her profile as indicated by consequently built, regular sub-groupings of companions, and at various levels of granularity [1]. As sharing individual media online winds up less demanding and broadly spread, new security concerns develop – particularly when the steady idea of the media and related setting uncovers insights about the physical and social setting in which the media things were made. we utilize setting mindful camera telephone gadgets to inspect protection choices in versatile and online photograph sharing. Through information investigation on a corpus of protection choices and related setting information from a certifiable framework, we recognize connections between area of photograph catch and photograph security settings, a few ramifications and open doors for plan of media sharing applications, including utilizing past security examples to forestall oversights and errors. [8] At the time we sent the review, Facebook enabled users to deal with the security settings of transferred (photographs, recordings, statuses, connections and notes) utilizing five unique granularities: Only Me, Specific People, Friends Only, Friends of Friends, and Everyone. Particular People enables users to unequivocally pick companions to impart substance to. The default or "suggested" protection setting [7]. We convey a review, actualized as a Facebook application, to 200 Facebook users we locate that 36% of substance stays imparted to the default protection settings. We likewise locate that, generally, protection settings coordinate users' desires just 37% of the time, and when off base, quite often open substance to a larger number of users than anticipated. At long last, we investigate how our outcomes can possibly help users in choosing suitable protection settings by inspecting the client made companion records. Most substance sharing s enable users to enter their security inclinations. Tragically, late examinations have demonstrated that users battle to set up and keep up such protection settings [2]. One of the principle reasons gave is that given the measure of shared data this procedure can be repetitive and mistake inclined. In this manner, numerous have recognized the need of approach suggestion systems which can help users to effortlessly and legitimately design security settings. Be that as it may, existing recommendations for robotizing protection settings give off an impression of being deficient to address he extraordinary security needs of images [3], because of the measure of data certainly conveyed inside images, and their association with the online condition wherein they are uncovered [6]. Well known photograph sharing sites have pulled in a great many users and helped develop gigantic social systems. Contributing images to an intrigue gathering would incredibly advance associations amongst users and extend their social systems. In this work, we mean to deliver programmed proposals of a users images to reasonable photograph sharing gatherings Photo sharing s, for example, Yahoo! Flickr® now permit and advance development of intrigue gatherings. In such gatherings, the connections normally include sharing pictures and recordings of or identified with the subjects of intrigue. Inside a huge social system, contributing images to at least one intrigue bunches is relied upon to enormously advance the individual social connections of users and extend their own social networks [9].

## III. A3P FRAMEWORK

### A. Preliminary Notions

Users can express their privacy preferences about their content disclosure preferences with their socially connected users via privacy policies. We define privacy policies according to Definition 1. Our policies are inspired 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, coworkers), or 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 “summer.jpg” before year 2012. Her privacy preferences can be expressed by the following policy:

P: ½{friend, coworker}, {vacation_album, summer.jpg}, {comment, tag}, (date< 2012)_.

### B. System Overview

The A3P system consists of two main components: A3P-core and A3P-social. The overall data flow is the following. 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:

1. The user does not have enough data for the type of the uploaded image to conduct policy prediction;
2. 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. Otherwise, the user can choose to revise the policy. The actual policy will be stored in the policy repository of the system for the policy prediction of future uploads.

## IV. 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 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. As for the one-stage mining approach, it would not be able to locate the right class of the new image because its classification criteria need both image features and policies whereas the policies of the new image are not available yet.

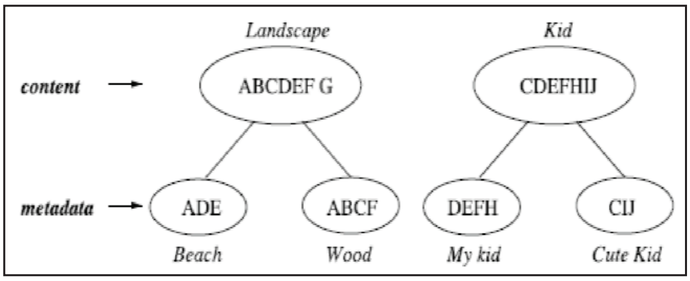

Fig. 1:

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.

### C. 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. Such a hierarchical classification gives a higher priority to image content and minimizes 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, 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 subcategories under each theme 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”.

### D. 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. Our selected similarity criteria include texture, symmetry, shape (radial symmetry and phase congruency [19]), and SIFT [15]. We also account for color and size. We set the system to start from five generic image classes: (a) explicit (e.g., nudity, violence, drinking etc), (b) adults, (c) kids, (d) scenery (e.g., beach, mountains), (e) animals. As a preprocessing step, we populate the five baseline classes by manually assigning to each class a number of images crawled from Google images, resulting in about 1,000 images per class. Having a large image data set beforehand reduces the chance of misclassification. Then, we generate signatures of all the images and store them in the database. Upon adjusting the settings of our content classifier, we conducted some preliminary test to evaluate its accuracy. Precisely, we tested our classifier it against a ground-truth data set, Image-net.org [17]. In Image-net, over 10 million images are collected and classified according to the wordnetstructure. For each image class, we use the first half set of images as the training data set and classify the next 800 images. The classification result was recorded as correct if the synset‟s main search term or the direct hypernym is returned as a class. The average accuracy of our classifier is above 94 percent. Having verified the accuracy of the classifier, we now discuss how it is used in the context of the A3P core. When a 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. To determine the class of the uploaded image, we find its first m closest matches. 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, to help refine future policy prediction. In our current prototype, m is set to 25 which is obtained using a small training data set.

## V. 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. As mentioned earlier, A3Psocial will be invoked by the A3P-core in two scenarios. One is when the user is a newbie of a site, and does not have enough images stored for the A3P-core to infer meaningful and customized policies. The other is when the system notices significant changes of privacy trend in the recommendation process.

### A. Analysis of Users’ Characteristics

We are also interested in examining whether our algorithm performs better for users with certain characteristics. Therefore, we study possible factors relevant to the performance of our algorithm. We used a least squares multiple regression analysis, regressing performance of the A3P-core to the following possible predictors:

- Frequency of social network use was measured on a frequency rating scale (1 ¼ daily; 2 ¼ weekly; 3 ¼ monthly; 4 ¼ rarely; 5 ¼ never) with the item "How often do you access Social Network Sites?".
- Privacy settings take time was measured on a LikertScale (5-point rating scale, where 1¼ strongly agree and 5 ¼ strongly disagree) with the item "Changing privacy settings for images uploaded on a social site can be very time consuming."
- Frequency of sharing pictures was measured using three items (a ¼ 0:69) rated on a Likert scale.
- Frequency of changing privacy settings was measured using four items (a ¼ 0:86) rated on a Likert scale.
- Privacy concern was measured using four items (a ¼ 0:76) rated on a Likert scale. An example item is "I have had concerns about my privacy due to shared images on social network sites."

The model results are shown in Table 5. We can observe that the content of concern variable was the biggest predictor of performance of our algorithm (standardized b ¼ 0:461, p < 0:001). This suggests the importance of content in determining the privacy level of uploaded images to social network sites. Privacy concern was also a significant predictor of performance (standardized b ¼ 0:329, p < 0:01) with increased performance for those users who felt that images uploaded to social network sites allowed for exposure of personal information. Surprisingly, none of the other predictors were significantly related to performance of the A3P-core. We expected that frequency of sharing pictures and frequency of changing privacy settings would be significantly related to performance, but the results indicate that the frequency of social network use, frequency of uploading images and frequency of changing settings are not related to the performance our algorithm obtains with privacy settings predictions. This is a particularly useful result as it indicates that our algorithm will perform equally well for users who frequently use and share images on social networks as well as for users who may have limited access or limited information to share.

In the second round of experiments, we analyze the performance of the A3P-Social component by using the first set of data collection. For each user, we use the A3PSocial to predict policies and compare it with a base-line which does not consider social contexts but bases recommendation only on social groups that have similar privacy strictness level for same type of images.

Using the base-line approach, we note that regardless of the individual privacy inclination of the users, the best accuracy is achieved in case of explicit images and images dominated by the appearance of children. In both cases, users maintain more consistent policies and our algorithm is able to learn them effectively. The largest variability, and therefore worse results occur for images denoting scenery, where the error rate is 15.2 percent.

Overall, the accuracy achieved by grouping users by strictness level is 86.4 percent. With A3P-Social, we achieve a much higher accuracy, demonstrating that just simply considering privacy inclination is not enough, and that "social-context" truly matters. Precisely the overall accuracy of A3P-social is above 95 percent. For 88.6 percent of the users, all predicted policies are correct, and the number of missed policies is 33 (for over 2,600 predictions). Also, we note that in this case, there is no significant difference across image types. For completeness, we compared the performance of the A3P-Social with alternative, popular, recommendation methods: Cosine and Pearson similarity [5]. Cosine similarity is a measure of similarity between two vectors of an inner product space that measures the cosine of the angle between them. In our case, the vectors are the users" attributes defining their social profile. The algorithm using Cosine similarity scans all users profiles, computes Cosine similarity of the social contexts between the new user and the existing users. Then, it finds the top two users with the highest similarity score with the candidate user and feeds the associated images to the remaining functions in the A3P-core.

Persons similarity instead measures how highly correlated are two variables, and is usually used to correlate users" ratings on recommended products. To adapt, we replaced the users rating from the Pearson similarity with self-given privacy ratings, that is, we tested similarity based on how users rate their own privacy inclinations. The data we use for this assumption is the response to three privacy-related questions users provide on their presession survey during data collection (the questions are adapted from the well-known privacy-index measures from Westin). Accordingly, we use Pearson similarity to find other users who are similar to this new user. With Pearson, we obtain an accuracy of 81.4 percent. We note however that 2-components accuracy is only about 1.77 percent of the missed policies, and even less 1-component. A similar result is obtained with Cosine similarity, where we achieved 82.56 percent accuracy, with again less than 2 percent accuracy for 2-components match and about 0.05 percent for 1-component. In sum, A3P social appears to be always superior to other methods. Note however that we cannot use A3P-social alone without A3P-core since the A3P-social does not factor in the evolution of an individuals privacy preferences.

Also A3P-social is more costly to be executed than A3P-core since the A3P-social analyzes information from a community rather than a single user.

## VI. Proposed Work

In this paper we suggest an alternative approach that Non-recommended user accessibility for particular image. At present other recommended users only can view all the features of an image whereas proposed system can be extended to view complete features of image.

The non-recommended user first request to admin, the admin may provide accessibility based on max count of image views. And user can search or view image details, User can send friend request to other friends.

It helps people in giving access for sharing information to other people and also helps people in restricting the access on some other information which cannot be made public.

Our friends can share the data so we use an meta data.

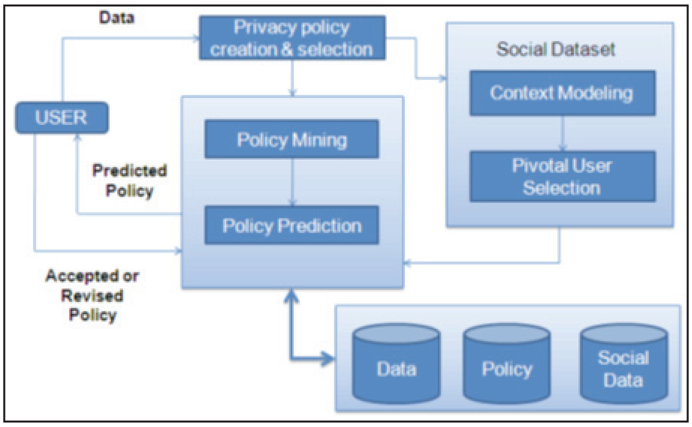

Fig. 1: Proposed Architecture

## VII. Results

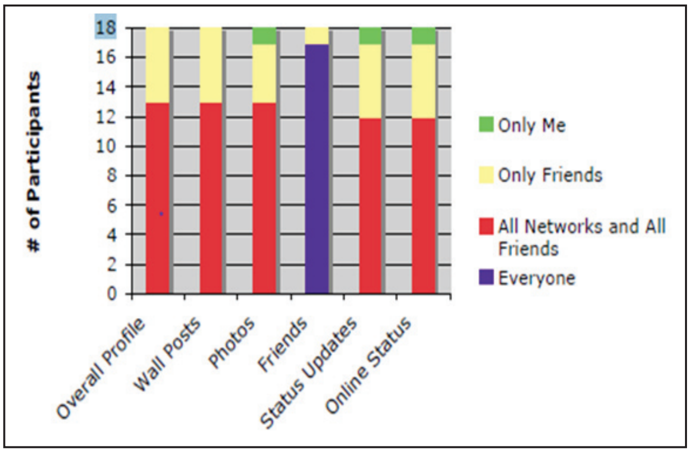

Fig. 2:

The A3P System in combined with the AIA which is implemented by using Java. The proposed will be tested on our own Image Set. The Metadata based classification will compare the tags with the already uploaded Images. The system predicts privacy policy accordingly. In the Content- Based Classification, features of the image will be extracted by using the SIFT Algorithm.

## VIII. Conclusion and Future Enhancement

We proposed a two-level framework which maintains user's available history on the site. In addition, in the system, non-recommended user can search and send the request of image to the administrator can accept the response and approve the access permissions. The results show the effectiveness of our concept classification and group/tag recommendation approaches. It provides a content sharing like text, image, audio, video, etc… With this emerging E-service for content sharing in social sites privacy is an important issue. It is an emerging service which provides a reliable communication, through this a new attack ground from an un-authored person can easily misuses the data through these media.

In Future use the BIC algorithm to classify the attackers and the users with the help of the Access Policy Prediction and Access control mechanism. These provide a privacy policy prediction and access restrictions along with blocking scheme for social sites and improve the privacy level for the user in social media.

## References

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

[2] K. Strater, H. Lipford,"Strategies and struggles with privacy in an online social networking community", In Proc. Brit. Comput. Soc. Conf. Human-Comput. Interact, pp.111–119, 2008.

[3] S.Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, R. Nair,"Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing", In Proc. Conf. Human Factors Comput. Syst., pp. 357–366, 2007.

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

[5] K. Nithya, N. Venkateswarulu,"A Two- Level Framework for Protecting the Privacy of User Uploaded images on Content Sharing Sites", [Online] Available: http://ijsetr.com/uploads/215634IJSETR12238-1463.pdf

[6] Anna Cinzia Squicciarini, Dan Lin, SmithaSundareswaran, Joshua Wede,"Privacy Policy Inference of UserUploaded Images on Content Sharing Sites", IEEE Transactions on Knowledge and Data Engineering, Vol. 27, No. 1, 2015.

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

[8] S.Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, R. Nair,"Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing", In Proc. Conf. Human Factors Comput. Syst., pp. 357–366, 2007.

[9] J. Yu, D. Joshi, J. Luo,"Connecting people in photo-sharing sites by photo content and user annotations", In Proc. IEEE Int. Conf. Multimedia Expo, pp. 1464–1467, 2009.

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

Ms. G. Kranthi, Pursuing M.Tech (CSE) from Avanthi Institute of Engineering and Technology, Vizianagaram, A.P. Received her B.Tech degree from Thandra Paparaya Institute of science & Technology, Komatipally, Bobbili, Vizaianagaram, Andhra Pradesh, India. She is actively participated in various workshops and seminars and presented papers related to information technology. Her area of interests are database management system and advanced computer applications.

Mr Kodanda Rama Swami Pursuing Ph.d from GITAM University, Received his M.Tech degree from GITAM University and M.sc from Andhra University, AP, India. Currently, he is working as Associate Professor, Department of CSE Avanthi Institute of Engineering and Technology, (Tagarapuvalasa), Visakhapatnam. He is having 11 years of teaching experience. His research interest includes Datamining, Database management system and Network security.