



Using Adaptive Privacy Policy Prediction (A3P) for improved Privacy of User Data and Images on Content Sharing

P. Harika¹, Addanki Kavitha²

¹Lecturer, Dept. of Computer Science, Sri Durga Malleswara Siddhartha Mahila kalasala, Vijayawada, A.P., India.

²Lecturer, Dept of Computer Science, P.B.Siddhartha College of Arts and Science, Vijayawada , A.P., India.

Abstract — A number of researchers have studied the social uses and privacy issues of online photo sharing or content sharing sites , but less have explored the privacy issues of photo sharing in social networks. Users of social-networking services share abundant information with numerous “friends.” This improved technology causes to privacy violation where the users are sharing the enormous volumes of images across more number of peoples. This privacy need to be taken care in order to make better the user satisfaction level. Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. Social networking sites such as Facebook, LinkedIn, etc give opportunities to share large amount of personal information. People upload their photos to these sites to gain public attention for social purposes, and thus many public consumer photographs are available online. The proliferation of personal data leads to privacy violation .Risks such as identify theft, embarrassment, and blackmail are faced by user’s .In order to overcome these risks flexible privacy mechanisms need to be considered. The main aim of this survey is to provide a review on different privacy policy approaches to enhance the security of personal information shared in the online social networking sites.

Keywords — *content sharing, Security, Online Social networking communities, user data.*

I. INTRODUCTION

Adaptive policy prediction. User images are first classified based on content and metadata. Privacy policies of each category of images are analyzed for the policy prediction. Content-based classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. Metadata-based classification groups images into subcategories under aforementioned baseline categories. A3P-social multi-criteria inference mechanism that generates representative policies by leveraging key information related to the user’s social context. Images searching for content based and image based the result found for each image privacy policy set of user privacy in sharing site. Contentbased classification is based on an

efficient and yet accurate image similarity approach. Classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. The Image encodes frequency and spatial information related to image color, size, and texture. The online social networking sites are the websites that enable users to join online communities, make new contacts, find old friends, and share common interests and ideas with large number of people across the world. It allows us to communicate with other internet users and build connections. The kinds and numbers of these content sharing sites have grown and participation of users also increased. As part of their participation lot amount of personal information are shared. The privacy policy of user uploaded data can be provided based on the personal characteristics. The privacy preferences of a user can be obtained from their profile information and relationships with others. The privacy policy of user uploaded image can be provided based on the content and meta data of user uploaded images. A hierarchical classification of images gives a higher priority to image content.

II .PROBLEM STATEMENT

For sensitive and risky information a solution to over-disclosures is to enforce, or at least default to, more restrictive settings. This may help new users by providing immediate protection, and it may also protect even experienced users while by allowing them to customize their settings to share information when desired. Sensitive information can appear in many profile areas, so new defaults may do not match the desires of users. Privacy controls also need to be more visible, making them accessible while users are modifying their profile instead of located on separate pages. If the user ignores these privacy pages, they will never see their options for modifying the privacy settings. There is a need to promote correct understanding of the audience of information we are sharing. For improving user’s awareness of their profile accessibility initially, certain mechanisms need to be introduced. Content sharing sites (CSS) such as Google+, Picasa, Facebook, and Twitter have become one of the fastest emerging e-

services. There are numerous issues affected these e-services like security and privacy. They where many advance projected for the privacy preserving policy for this social network. Some advance may cause problem since of unproductive algorithms. Many approaches were executed which failed to avoid the data exploitation and privacy problem. Most of the trouble we had studied in the existing system was acknowledged in terms of privacy and security of image data through the communication from one to an additional user in social network.

III .RELATED WORK

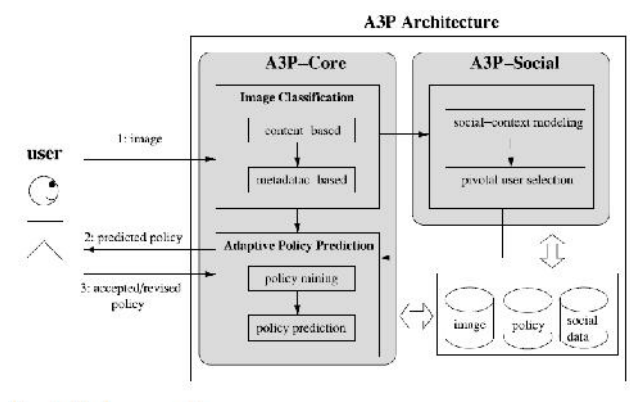
A3P SOCIAL : The A3P-social employs a multi-criteria inference mechanism that generates representative policies by leveraging key information related to the user's social context and his general attitude toward privacy. As mentioned earlier, A3Psocial will be invoked by the A3P-core in two scenarios. 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 user's social circle, which may be of interest for the user to possibly adjust his/her privacy settings accordingly. In what follows, we first present the types of social context considered by A3P Social, and then present the policy recommendation process. Users maintain more consistent policies, and our algorithm is able to teach them effectively. Images searching for content based and image based the result found for each image privacy policy set of user privacy in sharing site. Uploaded a new image and the A3P-core invoked the A3P-social for policy recommendation. The number of users in social network may be huge and that users may join a large number of social groups, it would be very time consuming to compare the new user's social context attributes against the frequent pattern of each social group.

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 twostage approach is more suitable for policy recommendation than applying the common onestage 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 twostage 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. 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.

A. Content-Based Classification: Content-based classification is based on an efficient and yet accurate image similarity approach. Classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. The Image encodes frequency and spatial information related to image color, size, and texture. The small number of coefficients is selected to form the signature of the image.

B. Metadata-Based Classification: The metadata-based classification groups images into subcategories under aforementioned baseline categories. Extract keywords from the metadata associated with an image metadata vector frequency find a subcategory that an image belongs to. This is an incremental procedure. The privacy approach with in same category of the new image user defines a policy same category of the new image, conduct association rule mining on the subject component of polices. Extract keywords from the metadata associated with an image. The metadata considered in our work are tags, captions, and comments. Retrieve the hyponym for each it a metadata vector. Select the hyponym with the highest frequency. Subcategory that an image belongs to, this is an incremental procedure. At the beginning, the first image forms a subcategory as itself and the representative hyponyms of the image becomes the subcategory's representative hyponyms. Compute the distance between representative hyponyms of a new incoming image and each existing subcategory.



IV. LITERATURE SURVEY

Author[1]: Fabeah Adu-Oppong et al. [2008] created idea of groups of friends. It gives an online answer for secure individual data. The method named Social Circles Finder, which consequently creates the companion's rundown. It is a procedure that examinations the group of friends of a man and recognizes the power of relationship and consequently groups of friends got an important classification of companions for setting protection approaches. The application will recognize the groups of friends of the subject however not indicate them to the subject. The subject will then be made inquiries about their eagerness to share a bit of their own data. In light of the answers the application finds the visual chart of clients.

Author[2]: Jonathan Anderson et al. [2009] proposed Privacy Suites which permits clients to effortlessly pick "suites" of security settings. A protection suite can be made by a specialist utilizing security programming. The security suite is disseminated through dispersion channels to the individuals from the social destinations. The disadvantage of a rich programming dialect is less understandability for end clients. Given an adequately abnormal state dialect and great coding hone, propelled clients ought to have the capacity to check a Privacy Suite. The primary objective is straightforwardness, which is vital for persuading compelling clients that it is protected to utilize.

Author[3]: Peter F. Klemperer et al. [2012] built up a tag based get to control of information partook in the web-based social networking destinations. A framework that creates get to control approaches from photograph administration labels. Each photograph is fused with a get to lattice for mapping the photograph with the client's companions. The members can choose an appropriate inclination and get to the data. Photograph labels can be separated as authoritative or informative in view of the client needs. There are a few critical confinements to our study outline. In the first place, our outcomes are constrained by the members we selected and the photographs they gave. A second arrangement of burdens concerns our utilization of machine created get to control rules. The calculation has no entrance to the unique situation and importance of labels and no knowledge into the strategy the member expected when labeling for get to control. Subsequently, a few guidelines seemed interesting to the members, conceivably driving them toward express arrangement based labels like "private" and "open."

V.CONCLUSION

In this paper , distinctive security strategy systems for client transferred information and pictures in substance sharing locales are portrayed in this paper. Picture substance and client conduct decides the protection strategy era. Display frameworks have certain points of interest and additionally hindrances. The A3P framework beats different techniques however it has a fault, that is when meta information data about transferred pictures are inaccessible it is hard to make security strategy. Future works prompt to consequently explaining pictures. Programmed picture comment is a testing issue in interactive media content examination and PC vision. To annotate images a hierarchical framework is used. An image-filtering algorithm to remove most of the irrelevant images for an unlabeled image is presented first. For the unlabeled image, an image cluster is allocated using a discriminative model as the primary relevant image set in the algorithm. In the second stage, a hybrid annotation model is proposed to annotate images. A baseline method is presented to transfer labels from relevant images to unlabeled image according to global visual features.

REFERENCES

1. H. Sundaram, L. Xie, M. De Choudhury, Y. Lin, and A. Natsev, "Multimedia semantics: Interactions between content and community," *Proc. IEEE*, vol. 100, no. 9, pp. 2737–2758, Sep. 2012.
2. J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in *Proc. Symp. Usable Privacy Security*, 2009.
3. 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.
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. 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.
6. A. Mazzia, K. LeFevre, and A. E., "The PViz comprehension tool for social network privacy settings," in *Proc. Symp. Usable Privacy Security*, 2012.
7. 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.