AN ADAPTIVE PRIVACY POLICY PREDICTION FRAMEWORK FOR UPLOADING IMAGES ON SOCIAL NETWORKS

***U. MOHAN SRINIVAS*,**

Assoc. Prof., Department of CSE & MCA, QIS College of Engineering and Technology, Ongole,

***K.V.BARGAV*,**

Final Year Student of Master of Computer Applications, QIS College of Engineering and Technology, Ongole

Abstract: *Photo sharing refers to the transfer or publishing of user's digital photos online and the website which provides such acquaintances offer services such as hosting, uploading, sharing and managing of photos through online system. With the expanding volume of pictures users share through social destinations, keeping up security has turned into a noteworthy issue, as shown by an ongoing flood of advanced episodes where clients incidentally shared individual data. In light of these occurrences, the need of devices to enable clients to control access to their mutual substance is evident. Toward tending to this need, we propose an Adaptive Privacy Policy Prediction (A3P) framework to enable clients to create security settings for their pictures. We propose a two-level structure which as per the client's accessible history on the site, decides the best accessible protection arrangement for the client's pictures being transferred. Our answer depends on a picture characterization structure for picture classifications which might be related with comparative approaches, and on a strategy forecast calculation to naturally produce an arrangement for each recently transferred picture, additionally as indicated by clients' social highlights. After some time, the produced approaches will pursue the development of clients' protection frame of mind. We give the after effects of our broad assessment more than 5,000 arrangements, which show the viability of our framework, with forecast exactnesses more than 90 percent.*

Keywords: Online information services, web-based services, picture characterization.

I. INTRODUCTION

Pictures are presently one of the key empowering agents of clients' network. Sharing happens both among already settled gatherings of known individuals or groups of friends (e.g., Google+, Flickr or Picasa), and furthermore progressively with individuals outside the clients groups of friends, for motivations behind social revelation to help them distinguish new associates and find out about companions interests and social environment. In any case, semantically rich pictures may uncover content delicate data. Consider a photograph of an understudy's 2012 graduation function, for instance. It could be shared inside a Google+ circle or Flickr bunch, however may pointlessly uncover the students BApos relatives and different companions. Sharing pictures inside online substance sharing destinations, subsequently, may rapidly prompt undesirable exposure and security infringement. Promote, the persevering way of online media makes it workable for different clients to gather rich collected data about the proprietor of the distributed substance and the subjects in the distributed substance. The collected data can bring about unforeseen presentation of one's social condition and prompt manhandle of one's close to home data. Further, the persistent nature of online media makes it possible for other users to collect rich aggregated information about the owner of the published content and the subjects in the published content [3], [1], [4]. 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 [2], recent studies have shown that users struggle to set up and maintain such privacy settings [1], [2], [5], [6]. 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 recommendation systems which can assist users to easily and properly configure privacy settings [7], [8], [9], [10]. However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images [13], [12], [11], due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed. In this paper, we propose an Adaptive Privacy Policy Prediction (A3P) system which aims to provide users a hassle free privacy settings experience by automatically [4], generating personalized policies. The A3P system handles user uploaded images, and factors in the following criteria that influence one's privacy settings of images: The impact of social environment and personal characteristics. Social context of users, such as their profile information and relationships with others may provide useful information regarding users' privacy preferences. For example, users interested in photography [14], may like to share their photos with other amateur photographers. Users who have several family members among their social contacts may share with them pictures related to family events. However, using common [15], policies across all users or across users with similar traits may be too simplistic and not satisfy individual preferences. Users may have drastically [16], different opinions even on the same type of images.

II RELATED WORK

2.1Imagined communities: Awareness, information sharing, and privacy on the Facebook.

Online informal organizations, for example, Friendster, MySpace, or the Facebook have encountered exponential development in enrollment as of late. These systems offer appealing means for between activity and correspondence additionally raise protection and security concerns [17]. In this review we study an agent test of the individuals from the Facebook (an interpersonal organization for universities and secondary schools) at a US scholastic establishment, and contrast the study information with data recovered from the net-work itself. We search for fundamental [18], statistic or behavioral differences between the groups of the system's individuals and non-individuals; we break down the effect of security worries on individuals' conduct; we contrast individuals' expressed demeanors and real conduct; and we archive the adjustments in conduct resulting to protection related data introduction.

2.2 A Survey on the Privacy Settings of User Data and Images on Content Sharing Sites

Online networkings turned out to be a standout amongst the most essential piece of our everyday life as it empowers us to speak with many individuals. Production of long range interpersonal communication locales, for example, MySpace, LinkedIn, and Facebook, people are offered chances to meet new individuals and companions [19], in their own particular and furthermore in the other assorted groups over the world. Clients of interpersonal interaction administrations [20], [18], [15], impart a wealth of individual data to an expansive number of "companions." This enhanced innovation prompts security infringement where the clients are sharing the huge volumes of pictures crosswise over more number of people groups. This protection should be taken care with a specific end goal to enhance the client fulfillment level.

2.3 Privacy Stories: Confidence in Privacy Behaviours through End User Programming

This paper exhibit, In the hunt to give clients important control over their data, we ought to consider End User Programming [18], [14], [17], methods as a conceivable swap for either obscure, master decided decisions or the perpetual expansion of choices that emerges from a short-sighted use of direct control [12], principles. We portray a work in advance to concentrate the suitability of this approach for enhancing the ease of use of interpersonal organization protection design. We make utilization of investigative convenience strategies to examine the ease of use difficulties of the current Facebook interface and to advise the outline of our proposed elective. We then give an account of a little (two-client) pilot study and take a gander at difficulties that we will address in future outline emphases.

2.4 Strategies and Struggles with Privacy in an Online Social Networking Community

Online long range informal communication groups, for example, Facebook and MySpace are to a great degree famous. These locales have changed what number of individuals create and keep up connections through posting and sharing individual data. The sum and profundity of these individual exposures have raised concerns in regards to online security. We develop past research on clients' under-use of accessible security alternatives by analyzing clients' ebb and flow systems for keeping up their protection, and where those methodologies bomb, on the online informal organization website Facebook. Our outcomes show the requirement for components that give familiarity with the security effect of clients' day by day collaborations

EXISTING SYSTEM

Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. 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 recommendation systems which can assist users to easily and properly configure privacy settings.

Disadvantage

❖ Sharing images within online content sharing sites, therefore, may quickly leadto unwanted disclosure and privacy violations.

❖ Further, the persistent nature of online media makes it possible for other users to collect rich aggregated information about the owner of the published content and the subjects in the published content.

❖ The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

III PROPOSED SYSTEM

In this paper, we propose an Adaptive Privacy Policy Prediction (A3P) system which aims to provide users a hassle free privacy settings experience by automatically generating personalized policies. The A3P system handles user uploaded images, and factors in the following criteria that influence one's privacy settings of images:

The impact of social environment and personal characteristics. Social context of users, such as their profile information and relationships with others may provide useful information regarding users' privacy preferences. For example, users interested in photography may like to share their photos with other amateur photographers. The role of image's content and metadata. In general, similar images often incur similar privacy preferences, especially when people appear in the images. For example, one may upload several photos of his kids and specify that only his family members are allowed to see these photos.

Advantages

The A3P-core focuses on analyzing each individual user's own images and metadata, while the A3P-Social offers a community perspective of privacy setting recommendations for a user's potential privacy improvement. We design the interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice.

IV METHODOLOGY

SYSTEM ARCHITECTURE

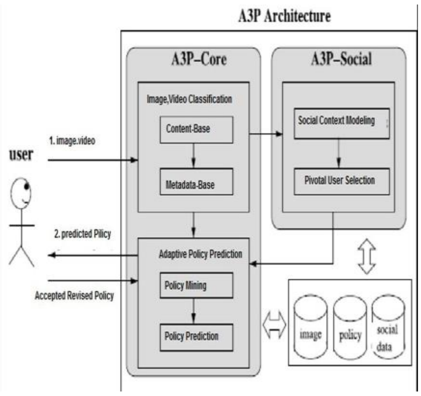

Fig: System Architecture

A. Content-Based Classification: it classifies image contents and then refines each category into subcategories with the help of hierarchical classification which gives higher priority to image content and minimizes the influence of missing tags.

B. Adaptive Policy Prediction: The policy prediction algorithm provides a predicted policy of a newly uploaded image to the user for his/her reference. More importantly, the predicted policy will reflect the possible changes of a user's privacy concerns.

Problem Statement:

Suppose user want to share any images and video so user may or may not want to share this data to all level, user must want to provide some assurance where user will place data and provide some type of security on traveling data. Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. 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 recommendation systems which can assist users to easily and properly configure privacy settings However, existing proposals for automating privacy settings appear to be inadequate 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.

a) A3P-CORE

b) A3P-SOCIAL *A3P-CORE:*

There are two major components in A3P-core: (i) Image, Video classification and (ii) Adaptive policy, predefined prediction. For each user, his/her images are first classified based on content and metadata. Then, privacy policies of each category of images and Video 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 Image classification: 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 do not have metadata will be grouped 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.

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”

The adaptive policy prediction process consists of three main phases: (i) policy normalization; (ii) policy mining; and (iii) policy prediction.

 Policy normalization: The policy normalization is a simple decomposition process to convert a user policy into a set of atomic rules in which the data (D) component is a single-element set.

 Policy mining: hierarchical mining first look for popular subjects defined by the user, then look for popular actions in the policies containing the popular subjects, and finally for popular conditions in the policies containing both popular subjects and conditions.

 Policy prediction: The policy mining phase may generate several candidate policies while the goal of our system is to return the most promising one to the user. Thus, we present an approach to choose the best candidate policy that follows the user’s privacy tendency. To model the user’s privacy tendency, we define a notion of strictness level. The strictness level is a quantitative metric that describes how “strict” a policy is.

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.

Social Context Modeling: The social context modeling algorithm consists of two major steps. The first step is to identify and formalize potentially important factors that may be informative of one’s privacy settings. The second step is to group users based on the identified factors.

Contribution:-

Base Paper is focus on the image data only. Base paper provides the facility of Image policy mining in the form of Subject (Whom), Action (Action perform), Condition (Time period). A new approach we also consider images as well as video data. (Refer architecture).Because video is more integral part on social media, Because of Increasing a ration of Mobiles phones user are taking very high interest into capture and upload video, So consider this point we Providing a Privacy Policy Inference of User-Uploaded Images and Video on Content Sharing Sites. To this contribution we are focus on the user uploads videos and predict policy to this video with using our architecture.

Algorithms:

There are two algorithms proposed as

Policy Prediction Algorithm.

Data mining Algorithm.

a. Select Dataset (News Dataset)

b. Preprocessing Data

c. Remove Stopword

d. Stamming Data

e. Find Out Term(Related Name Entities)

f. Match Data On Terms Basis

g. Select Matching friends nm

Image Comparison Algorithm:

There are many scenarios where tried to compare images but failed to compare them. Image comparison is a very deep concept where there involved lot many complex algorithms. In brief for Two images to be same we need to compare the two images pixel by pixel so i came across Pixel Grabber class in java and started using it which gave a positive result, but not accurate.

1. Select Image

Convert image into bitmap

Select target image to matching from friend list (profile) Convert into bitmap

2. Convert bitmap into byte array

3. Sort both bite array in basis of bytes

4. Compare every bit of byte array

If both array match then select matching profile of friend into policy.

OpenCv Algorithm for Face recognition-Pre-process the image, if needed (e.g. to enhance contrast, filter noise, etc.).

An Image Segmentation, process in which the image is converted to regions which contains pixels that are similar to pixels in the same region and different from pixels to other regions. This can be done using region-growing, mathematical morphology, clustering or classification algorithms. There are many algorithms to do that, just google for "image segmentation" and other keywords to get more information.

With the regions, create descriptors for them. Descriptors are calculated from the region and can include shape, area, perimeter, number of holes, general color of the region, texture, orientation, position, etc.

If needed, do a Re-Segmentation of the image, process in which regions are merged if they can be considered as belonging to the same object. Note that this step may require some high-level knowledge of the objects and the task in general, seldom being fully automatic and often being task-dependent.

If needed, filter the regions that seem relevant to the task in hand, eliminating small regions or regions which are deemed unrelated to the task (again this may require some knowledge about the task). Store the image's regions' descriptor for further processing.

Repeat those steps for other images.

Use the descriptors for comparison of the contents of the images, using some of many algorithms for pattern matching.

V CONCLUSION

An algorithm creates new framework for Images and Videos that are uploaded on Social site. Social network is an upgrading media for information sharing through internet. 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. This algorithm provides a predefined or automated privacy prediction policy where user gets Subject(To whom Data will be share), Action(What action will be performed by selected user i.e. Comment, View, Download) and Condition(Time period on which action should be perform) for Uploaded images or videos which 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.

VI 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] R. Agrawal and R. Srikant,“Fast algorithms for mining association rules in large databases,” in Proc. 20th Int. Conf. Very Large Data Bases, 1994, pp. 487–499.

[3] 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.

[4] M. Ames and M. Naaman, “Why we tag: Motivations for annotation in mobile and online media,” in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 971–980.

[5] 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.

[6] D. G. Altman and J. M. Bland ,“Multiple significance tests: The bonferroni method,” Brit. Med. J., vol. 310, no. 6973, 1995.

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

[8] 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.

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

[10] 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.

[11] 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.

[12] R. da Silva Torres and A. Falc~ao, “Content-based image retrieval: Theory and applications,” Revista de Inform_atica Te_orica e Aplicada, vol. 2, no. 13, pp. 161–185, 2006.

[13] R. Datta, D. Joshi, J. Li, and J. Wang, “Image retrieval: Ideas, influences, and trends of the new age,” ACM Comput. Surv., vol. 40, no. 2, p. 5, 2008.

[14] J. Deng, A. C. Berg, K. Li, and L. Fei-Fei, “What does classifying more than 10,000 image categories tell us?” in Proc. 11th Eur. Conf. Comput. Vis.: Part V, 2010, pp.71–84.[Online].Available: http://portal.acm.org/citation.cfm?id=1888150.1888157

[15] 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.

[16] L. Geng and H. J. Hamilton, “Interestingness measures for data mining: A survey,” ACM Comput. Surv., vol. 38, no. 3, p. 9, 2006.

[17] Image-net data set. [Online]. Available: www.image-net.org, Dec. 2013.

[18] S. Jones and E. O’Neill, “Contextual dynamics of group-based sharing decisions,” in Proc. Conf. Human Factors Comput. Syst., 2011, pp. 1777–1786.[Online].vailable:http://doi.acm.org/10.1145/1978942.1979200

[19] 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. 99615.94.

[20] A. Kaw and E. Kalu, Numerical Methods with Applications: Abridged., Raleigh, North Carolina, USA: Lulu.com, 2010.