International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 9 – DECEMBER 2016.

A SECURE ENHANCED PRIVACY POLICY IN CONTENT SHARING SITES USING FACE-TO-FACE KEY DISTRIBUTION SCHEME

MOHAMMAD MUNEERUDDIN[#1] and SHEIK AHMAD SHAH[*2]

[#] *PG Scholar, Kakinada Institute Of Engineering & Technology Department of Computer Science , JNTUK,A.P, India.*

[*] *Assistant Prof, Dept of CSE, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA.*

***Abstract*— Presently, the images are uploaded to the social sites in vast amount. Hence, privacy becomes an important issue in the content sharing sites. The users are unaware about their information shared in publicized environment. In this paper, we make a study about the privacy issue in the content sharing sites. We propose Adaptive Privacy Policy Prediction (A3P) that ensures the user's privacy settings for their images. The user's uploaded images are categorized based on their privacy settings. The prediction algorithm is used for mining the similar policies. Experimental results prove the efficiency of the systems.**

***Index Terms*— Images, Privacy, content sharing sites, privacy level and efficiency.**

I. INTRODUCTION

Images are now one of the key empowering agents of clients' connectivity. Image sharing occurs in both social groups as well as people from outside social circles [1]. Consider instances like Google +, Flickr or Picasa; it is mostly used for sharing the images with other users. The uploaded images are stored in semantic relationships. These semantically build images reveal their sensitive information. Sharing our images to the media sites may lead to unwanted disclosure and privacy violations [2]. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information. In most of the scenario, the user specifies their privacy preferences.

In current scenario, the users don't hold a single account in media environments. They hold higher number of accounts in various Online Social Networks. Let us assume that Alice and Bob belong to the same online social network OSN1 [3]. Bob can easily download a photo from Alice's profile, obviously without Alice's consent or any kind of notification. Bob can make several alterations on Alice's photo offline, and then share it in another online social network OSN2 [4]. It is clear that Alice will not be notified of the incident and no matter what privacy policies she has set on the photo, they will be bypassed.

The rest of the paper is organized as follows: Section I describe the current scenario of the OSNs; Section II describes existing works of research study; Section III discusses about the proposed work; Section IV justifies the proposed framework by doing experimental designs; Atlast concludes in Section V.

I. RELATED WORK

This section presents the existing studies conducted by various researchers in Online Social Networks (OSN).The users enclose different sorts of images to the social environment with the basic security level. Privacy management is the most vital part of social environment. Initially, we investigated about the interface usability of the social environment. The author [5] presented the analysis over profile information to percept the privacy settings. The author in [6] studied about building the semantic relationship for the collaborative environment. A recommendation based collaborative techniques build that creates recommended groups for the Flickr users. They created three memory based models and four model based models. The result shows that the model based systems exhibited higher efficiency than the memory based systems. Then the tag oriented image classification [7] system is derived for the sparse data.

To this end, we begin with analysing user annotations and modeling the shared images in a group. Both visual content and annotation context are then integrated to understand the events or topics depicted in those images [8].Our results demonstrate the need for mechanisms that provide awareness of the privacy impact of users‟ daily interactions. Profile Features Facebook profiles can be extensive, including a variety of self reported information (disclosures) as well as details of the user's social environment, including pictures, friends lists, and messages with friends[5].

Then the study is further enhanced using local radial symmetry that enhances the region of interest within the

image. Using some facial detector, generic region of the face is detected. Some superior performance of the system is employed in both computation complexity of the system. The refining process is studied for the visual similarity and semantic similarity. An image retagging scheme that aims at improving the quality of the tags associated with social images in terms of content relevance.

II. PROPOSED FRAMEWORK

The proposed framework executes in four phases, namely,

A. *System Construction Module*

The Adaptive Privacy Policy Protection (A3P) comprised of two parts: i) A3P Core and ii) A3P social. The A3P core is the first step in the system. If a user uploads an image, it will be transferred to the A3P core. The image is classified in A3P core and then checked for the image invocation in A3P social. Relied upon the user behavior, the user policy is defined. The A3P social is invoked by the A3P core when below two cases is proved true,

a) Insufficient data provided for the user uploaded image to process the policy prediction.

b) Discovery of privacy changes obtained among the user's community.

B. *Content-Based Classification*

In order to receive a cluster of images with same privacy preferences, a novel hierarchical image classification is framed. Firstly, the image is classified based on the content. Each classified image is then categorized and sub-categorized onto their metadata. Some images are grouped based on their content in absence of metadata. This type of image classification picks the content in higher priority and lessened the missing tags. It efficiently depicts the accurate image similarity model. The Haar Wavelet transformation is used for the comparison of the image signatures. The use of wavelet transform inscribes the information in view of frequency and spatial. The image signature is formed by the small number of wavelet coefficients. The distance function is used for obtaining the content similarity.

C. *etadata-Based Classification*

Depending upon the categories, the image is classified from groups to the subcategories using metadata. It comprised of three steps:

i) The keyword is filtered from the image enveloped in metadata. The metadata may include tags, captions and comments.

ii) A representative hypernym symbolized as h in each metadata vector is obtained.

iii) Then the discovery of image subcategory is the third step. Thus, it belongs to the function of incremental procedure.

D. *Adaptive Policy Prediction*

Every newly uploaded image is utilized for predicting the privacy policy based on user's references. The processes involved in the prediction are the a) Normalization of the policy, b) Mining the policy and c) Prediction of policy.

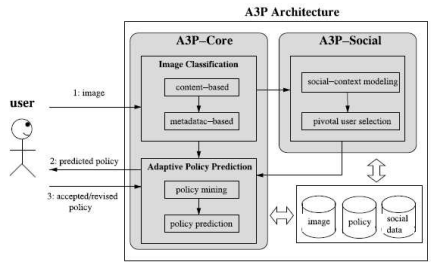

Fig.3.1 System architecture

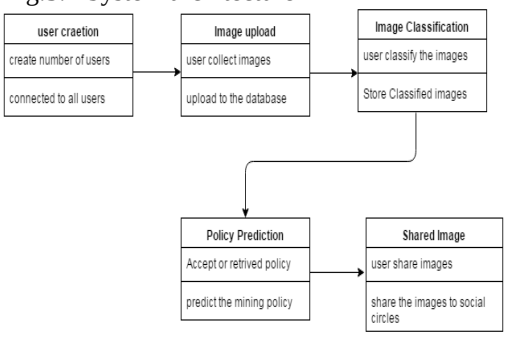

Fig.3.2 Class diagram for each users

III. EXPERIMENTAL DESIGNS

The proposed framework is deployed using Graphical User Interface (GUI) developed from Java platform.

Fig. 4.1 User's registration page with any online social networks

Fig.4.2 Login page of the User

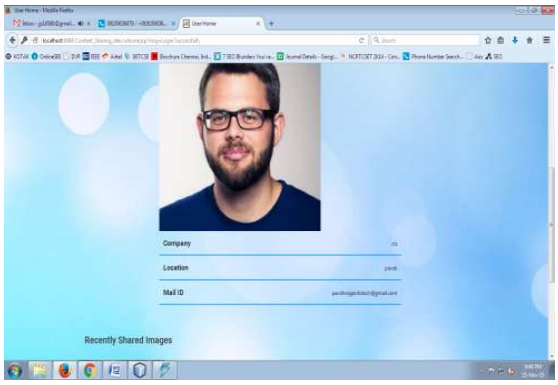

Fig.4.3 User viewing his profile from his login

Fig.4.4 User viewing the recently shared images

Fig.4.5 User sharing the images by entering the basic information details

Fig.4.6 Viewing the requested details

Fig.4.7 User's viewing the images shared by others

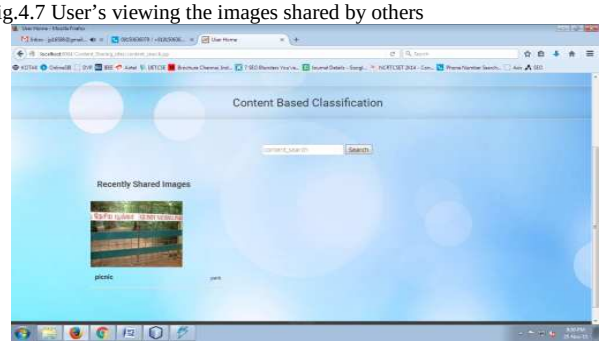

Fig.4.8 Images are classified based on the content classification system

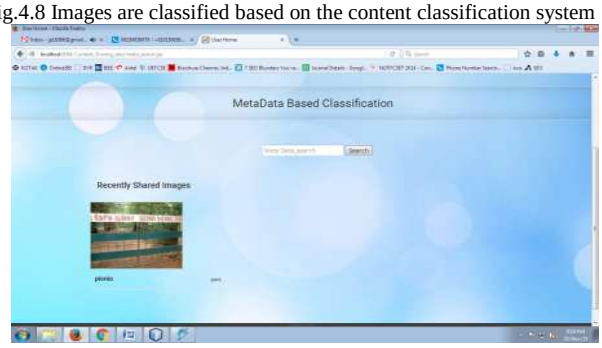

Fig.4.9 Images are classified based on the metadata based classification

IV. CONCLUSION

In this paper, we have framed a novel algorithm named, "Adaptive Privacy Policy Prediction (A3P)". The objective of the A3P is to automatically define the privacy policy settings for the user uploaded images. The privacy preference is seated upon the information generated for the intended user. The issues like cold-start, social context information are efficiently tackled. The A3P is developed as a practical tool that gains developments to the privacy. Experimental design shows the effectiveness of the systems.

REFERENCES

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

[2] N. Zheng, Q. Li, S. Liao, and L. Zhang, "Which photo groups should I choose? A comparative study of recommendation algorithms in flickr," J. Inform. Sci., vol. 36, pp. 733–750, Dec. 2010.

[3] 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.

[4] C.-H. Yeh, Y.-C. Ho, B. A. Barsky, and M. Ouhyoung, "Personalized photograph ranking and selection system," in Proc.Int. Conf. Multimedia, 2010, pp. 211–220. [Online]. Available: http://doi.acm.org/10.1145/1873951.1873963.

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

[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 G. Danezis, "Prying data out of a social network," in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining.,2009, pp.249– 254.

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

[9] M. Rabbath, P. Sandhaus, and S. Boll, "Analysing Facebook features to support event detection for photo-based facebook applications," in Proc. 2nd ACM Int. Conf. Multimedia Retrieval, 2012, pp. 11:1–11:8.

[10] Dan Lin, Sundareswaran.S, Wede.J,"Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites" in Proc. IEEE Int. Volume.27, Issue.1Jan. 1 2015

AUTHOR PROFILE

MOHAMMAD MUNEERUDDIN is a student of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada pursuing M.Tech (Computer Science). His Area of interest includes Data Mining and its objectives in all current trends and techniques in Computer Science.

SHEIK AHMAD SHAH M.TECH (UCE,JNTUK) is working as Assistant Professor, Department of Computer Science & Engineering, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA. His interested areas NETWOKING SECURITY.