A REVIEW OF VARIOUS PRIVACY POLICY APPROACHES TO IMPROVE SECURITY IN SOCIAL NETWORKING COMMUNITIES

Ashita

Abstract— **In recent years online social networking communities have undergone massive explosion. The number of sites as well as kinds of sites have grown and it allows us to communicate with a lot of people across the world. Social networking sites such as Facebook , Flickr, MySpace and LinkedIn, 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.**

***Index Terms*—Meta data, Online Social networking communities, Privacy Policy, Security,**

I. INTRODUCTION

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.

Particularly young internet users share private images about themselves, their friends and classmates without being aware of the consequences. Photo sharing users often lack awareness of privacy issues. Many photos publicly shared by young people are of such a private nature that they would not show these images to their parents and teachers. A variety of risks are faced by individuals, such as identify theft, stalking, embarrassment, and blackmail as a result of proliferation of personal data .Despite these risks, many privacy mechanisms of content sharing sites are very weak.

Manuscript received December, 2015.
***Ashita** , Department of Computer Science, KMCT College of Engineering, Calicut, Kerala.*

There is a need to develop more security features in online social networks. Privacy is critical feature among the security mechanisms. In some situations, we like to share information only to best friends, family members and in other instances we like to share with strangers also. Existing sharing platforms do not support users in making adequate privacy decisions in multimedia resource sharing. On the contrary, these platforms quite often employ rather lax default configurations, and mostly require users to manually decide on privacy settings for each single resource. Given the amount of shared information this process can be tedious and error-prone [1].

To address the unique privacy needs of images existing proposals for automating privacy settings are inadequate. A definition of internet privacy is it involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the internet. Internet privacy is a subset of data privacy. Privacy concerns have been articulated from the beginnings of large scale computer sharing. The privacy of user data can be given in two ways. 1. The user can enter the privacy preferences alone 2.Usage of recommendation systems which assist users for setting the privacy preferences.

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. PRIVACY CONCERNS WITH SOCIAL NETWORKING SITES

Privacy concerns with social networking services is a subset of data privacy, involving the binding personal privacy concerning storing, re-purposing, provision to third parties, and displaying of information through the Internet. Each day these sites process large amount of information. In order to gain access of other user's private information features like messages, invitations, photos, open platform application other applications are helpful. In the case of Facebook privacy features are weak .Various level of privacy are

ISSN: 2278 – 1323

offered by these sites. There are even sites in which user doesn't reveal their actual names. It is also possible for users to block other users. Most users do not realize that while they may make use of the security features on Facebook the default setting is restored after each update.

The privacy strategies introduced by our participants may have initially achieved desired privacy protection and matched their initial mental models of audience and accessibility, but these strategies often failed now due to excessive use.

When making decisions regarding the disclosure of information and privacy, users who are new to Facebook do appear to consider the possibility of a broad and public audience and take into consideration the range of people who might access their profiles. The perception of online audience appears to shrink, as users continue to explore the Facebook interface, enlarge their social networks, and interact with their friends through these sites.

It is also reported a variety of problems due to lack of usability of Facebook privacy settings. An accidental disclosure that is very difficult for users to detect happens when user's expectations of the outcome of their privacy settings did not match what actually happened. They rarely revisit their privacy pages to ensure settings appropriately cover the growing profile as they continue to expand their profiles by downloading new applications, joining new networks, or disclosing new information.

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. These mechanisms need to be attached to the regular activities of the users, so privacy does not remain a separate and rare consideration as the user's audience perceptions change.

III. LITERATURE SURVEY

Based on the concept of **social circles [2]** privacy settings were introduced by Fabeah Adu-Oppong. To protect personal information web based solution is provided. The technique named Social Circles Finder automatically generates the friend's list. It is a technique that analyses the social circle of a person and identifies the intensity of relationship and therefore social circles provide a meaningful categorization of friends for setting privacy policies. This technique will allow the subject identify the social circles but not show them to the subject. The willingness of subject to share a piece of their personal information will be asked. The application finds the visual graph of users based on the answers.

PViz Comprehension Tool [3], an interface and system that corresponds more directly with how users model groups and privacy policies applied to their networks was developed by Alessandra Mazzia . According to automatically-constructed, natural sub-groupings of friends, and at different levels of granularity PViz allows the user to understand the visibility of her profile. PViz is better than other current policy comprehension tools Facebook's Audience View and Custom Settings page. It also addresses the important sub-problem of producing effective group labels since the user must be able to identify and distinguish automatically-constructed groups.

Privacy Suites [4] is proposed by Jonathan Anderson which allows users to easily choose "suites" of privacy settings. Using privacy programming a privacy suite can be created by an expert. Privacy Suites could also be created directly through existing configuration UIs or exporting them to the abstract format. To the members of the social sites the privacy suite is distributed through existing distribution channels. Transparency is the main goal, which is essential for convincing influential users that it is safe to use. The disadvantage of a rich programming language is less understandability for end users. To verify a Privacy Suite sufficiently high-level language and good coding practice, motivated users are able.

Privacy-Aware Image Classification and Search [1] is a technique to automatically detect private images, and to enable privacy-oriented image search introduced by Sergej Zerr. To provide security policies technique combines textual meta data images with variety of visual features. It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game. In this the selected image features (edges, faces, color histograms) which can help discriminate between natural and man-made objects/scenes (the EDCV feature) that can indicate the presence or absence of particular objects (SIFT).

A tag based access control of data [5] is developed by Peter F. Klemperer. It is a system that creates access-control policies from photo management tags. Every photo is incorporated with an access grid for mapping the photo with the participant's friends. A suitable preference can be selected by participants and access the information. Based on the user needs photo tags can be categorized as organizational or communicative. There are several important limitations .First, our results are limited by the participants recruited and the photos provided by them. Machine generated access-control rules are the second limitation. Algorithm used here has no access to the context and meaning of tags and no insight into the policy the participant intended when tagging for access control. Hence, some rules appeared strange to the participants who makes them to tag explicitly like "private" and "public.

YourPrivacyProtector [6] is a recommender system proposed by Kambiz Ghazinour that understands the social internet behavior of their privacy settings and recommending reasonable privacy options. The parameters used are user's personal profile, User's interests and User's privacy settings on photo albums .With the help of these parameters the

ISSN: 2278 – 1323

system constructs the personal profile of the user. For a given profile of users it will automatically learn and assign the privacy options. It detects the possible privacy risks and allows users to see their current privacy settings on their social network profile, namely Facebook, and monitors frequently. Necessary privacy settings are adopted based on these risks.

A decentralised authentication protocol [7], is a access control system proposed by Ching-man Au Yeung based on a descriptive tags and linked data of social networks in the Semantic websites. Here users can specify access control rules based on open linked data provided by other parties and it allows users to create expressive policies for their photos stored in one or more photo sharing.

Adaptive Privacy Policy Prediction (A3P) [8] system is introduced by Anna Cinzia Squicciarini. Personalized policies can be automatically generated by this system. It makes use of the uploaded images by users and a hierarchical image classification is done. Images content and metadata is handled by the A3P system .It consists of two components: A3P Core and A3P Social. The image will be first sent to the A3P-core, when the user uploads the image. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social.When meta data information is unavailable it is difficult to generate accurate privacy policy. This is the disadvantage of this system. Privacy violation as well as inaccurate classification will be the after effect of manual creation of meta data log information.

IV. COMPARISON OF EXISTING METHODS

Paper: Social circles:-Tackling privacy in social networks.
Author: A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P.P.Tsang
Technique: Social Circles Finder
Advantage: Clarity
Disadvantage: Less user applicability

Paper: The PViz Comprehension Tool for Social Network Privacy Settings
Author: Alessandra Mazzia Kristen, LeFevre, and Eyta Adar
Technique: PViz Comprehension Tool
Advantage: User flexibility
Disadvantage: Less user understandability

Paper: Privacy suites- Shared privacy for social networks
Author: J. Bonneau, J.Anderson, and L. Church
Technique: Privacy Suite
Advantage: Clarity
Disadvantage: Less user understandability

Paper: I Know What You Did Last Summer! :Privacy-Aware Image Classification and Search
Author: Sergej Zerr,Stefan Siersdorfer
Technique: Privacy-Aware Image Classification and Search
Advantage: Directly search for private data
Disadvantage: Complexity

Paper: Tag, You Can See It! Using Tags for Access Control in Photo Sharing
Author: Peter F.Klemperer, Yuan Liang, Michelle L. Mazurek
Technique: Tags and linked data
Advantage: Clarity
Disadvantage: Less user applicability

Paper: Your privacy protector- A Recommender System For Privacy Settings in Social Networks
Author: Kambiz Ghazinour,Stan Matwinand,and Marina Sokolova
Technique: Your privacy protector
Advantage: Clarity
Disadvantage: Less user understandability

Paper: Decentralization- The future of online social networking
Author: Ching-man AuYeung
Technique: Tags and linked data
Advantage: Applicable to multiple content sharing sites
Disadvantage: Less user applicability

Paper: Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites
Author: Anna Cinzia Squicciarini
Technique: Adaptive policy prediction.
Advantage: Easy to understand.
Disadvantage: Difficulty in policy generation
In the case of unavailable meta data information.

V. CONCLUSION AND FUTURE WORKS

Various privacy policy techniques for user uploaded data and images in content sharing sites are described in this paper. Image content and user behavior determines the privacy policy generation. Present systems have certain advantages as well as disadvantages. The A3P system outperforms other methods but it has a demerit, that is when meta data information about uploaded images are unavailable it is difficult to create privacy policy. Future works lead to automatically annotating images.

Automatic image annotation is a challenging problem in multimedia content analysis and computer 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. Regional visual features are extracted to build a probabilistic model for image annotation. Finally, the two annotation results are fused together by a simple weighted algorithm. Experiments have proved this method will provide better results.

ISSN: 2278 – 1323

REFERENCES

[1] Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova , "I Know What You Did Last Summer !:Privacy-Aware Image Classification and Search", Proceedings of the 35th International ACM SIGIR conference on Research and development in information retrieval, 2012.

[2] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P.Tsang, "Social circles: Tackling privacy in social networks," in Proc. Symp. Sable Privacy Security, 2008.

[3] Alessandra Mazzia Kristen LeFevre and Eytan Adar, The PViz Comprehension Tool for Social Network Privacy Settings, Tech. rep., University of Michigan, 2011.

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

.

[5] Peter F. Klemperer, Yuan Liang, Michelle L. Mazurek, "Tag, You Can See It! Using Tags for Access Control in Photo Sharing", Conference on Human factors in Computing Systems, May 2012.

[6] Kambiz Ghazinour, Stan Matwin and Marina Sokolova, Social "Yourprivacyprotector: A Recommender System For Privacy Settings In Social Networks", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 4, August 2013.

[7] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linkeddata," in Proc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp. 9–14.

[8] 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.

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

[10] Yuan-yuan ca., Zhi-chun mu, Yan-fei ren ,and Guo-qing xu "A Hybrid Hierarchical Framework For Automatic Image Annotation" in Proc of the 2014 International Conference on Machine Learning and Cybernetics, Lanzhou, 13-16 July, 2014

Ashita, is a M.Tech student in Computer Science Department, KMCT College of Engineering under Calicut University, India.. She received B.Tech degree in 2014 from Calicut University, India. Her research interests are Data mining, computer networks etc.

ISSN: 2278 – 1323