Abstract

Nowadays Social media’s become extremely popular. It allows us to communicate with a lot of people. Creation of social networking sites such as LinkedIn, and Facebook, individuals are given opportunities to meet new people and friends across the world. Users of social-networking services share a large volume of personal information with a large number of “friends.” In a case where the users are sharing the large volumes of images across more number of people in that case this improved technology leads to privacy violation. This privacy need to be taken care in order to improve the user satisfaction level. The goal of this survey is to provide a complete review of various privacy policy methods to improve the security of information shared in the social media sites.

Keywords: Content sharing sites, Social media, privacy

1. Introduction

Online social networks allow users to build connections and relations to other Internet users. Social networks store information distantly, rather than on a user’s personal computer. Social networking can be used to keep in touch with friends, make new connections and find people with similar interests and ideas.

More security mechanisms are need to be develop for online social networks. Privacy is essential to the design of security mechanisms. Most social networks providers have offered privacy settings to permit or deny others access to personal information details. In certain occasions we want to share the information about ourselves only by a small circle of close Friends, and not by strangers. In other instances, we are willing to reveal private information to anonymous outsiders, but not to those who know us better.

Internet privacy means the ability to control [1] what information one reveals about oneself, and [2] who can access that information. Essentially, when the data is collected or analyzed without the knowledge or approval of its owner, privacy is violated. When it comes to the usage of the data, the owner should be informed about the purposes and intentions for which the data is being or will be used. Most content sharing sites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings [1], [9]. One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone [10], [11]. Therefore, many have acknowledged the need of policy recommendation systems which can support users to easily and properly configure privacy settings [2], [4], [12]. However, existing proposals for automating privacy settings appear to be insufficient to address the unique privacy needs of images, [5] due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed.

The privacy of user data can be given by using two methods. 1. The user alone can enter the privacy preferences 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 user 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. The privacy policy of user uploaded image can be provided based on the user uploaded image’s content and metadata. A hierarchical image classification which classifies images first based on their contents and then refine each category into subgroups 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.

2. Literature survey

Anna Cinzia Squicciarini developed an Adaptive Privacy Policy Prediction (A3P) [1] system, a free privacy settings system by automatically generating personalized policies. The A3P system handles user uploaded images based on the person’s personal characteristics and images content and metadata. The A3P system consists of two components: A3P Core and A3P Social. 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. The disadvantage is inaccurate privacy policy generation in case of the absence of metadata information about the images. Also manual creation of metadata log data information leads to inaccurate classification and also privacy violation.

Jonathan Anderson proposed a paradigm called Privacy Suites [7] which allows users to easily choose “suites” of privacy settings. A privacy suite can be created by professional using privacy programming. Privacy Suites could also be created directly through existing configuration UIDs or exporting them to the abstract format. The privacy suite is distributed through existing distribution channels to the members of the social sites. The drawback of a rich programming language is less understandability for end users. Given a satisfactorily high-level language and good coding practice, motivated users should be able to verify a Privacy Suite. The main goal is transparency, which is essential for convincing influential users that it is safe to use.

Fabeah Adu-Opong developed privacy settings based on the concept of social circles [8]. It provides a web based solution to protect personal information. 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. The application will identify the social circles of the subject but not show them to the subject. The subject will then be asked questions about their willingness to share a part of their personal information. Based on the answers the application finds the visual graph of users.

Kambiz Ghazinour designed a recommender system known as YourPrivacyProtector [2] that understands the social net behaviour of their privacy settings and recommending reasonable privacy options. It uses user’s personal profile, User’s interests and User’s privacy settings on photo albums as parameters and with the help of these parameters the system constructs the personal profile of the user. It automatically learned for a given profile of users and assigns the privacy choices. It allows users to see their current privacy settings on their social network profile, namely Facebook, and monitors and detects the possible privacy risks. Based on the risks it adopts the necessary privacy settings.

Alessandra Mazzia introduced PViz Comprehension Tool [5], an interface and system that corresponds more directly with how users model groups and privacy policies applied to their networks. PViz allows the user to understand the visibility of her profile according to automatically-constructed, natural sub-groupings of friends, and at different levels of granularity. Because the user must be able to identify and differentiate automatically-constructed groups, we also address the important sub-problem of producing effective group labels. PViz is better than other current policy conception tools Facebook’s Audience View and Custom Settings page.

Peter F. Klemperer established a tag based access control of data [4] shared in the social media sites. A system that creates access-control policies from photo management tags. Every photo is incorporated with an access grid for mapping the photograph with the participant’s friends. The members can choose a suitable preference and access the information. Photo tags can be categorized as organizational or communicative based on the user needs. There are several important limitations to our study design. First, our results are limited by the participants we recruited and the photos they provided. A second set of limitations concerns our use of machine generated access-control rules. The algorithm has no access to the context and meaning of tags and no insight into the policy the participant intended when tagging for access control. As a result, some rules appeared strange or arbitrary to the participants, potentially driving them toward explicit policy-based tags like “private” and “public”.

Ching-man Au Yeung propose a access control system based on a decentralized authentication protocol [6], descriptive tags and linked data of social networks in the Semantic Web. It allows users to create expressive policies for their photographs stored in one or more photo sharing sites, and users can specify access control rules based on open linked data provided by other parties.
Sergej Zerr proposes a technique Privacy-Aware Image Classification and Search [3] to automatically detect private images, and to enable privacy-oriented image search. It combines textual and metadata images with variety of visual features to provide security policies. In this the selected image features like edges, faces, color histograms which can help discriminate between natural and man-made objects/scenes like the EDCV feature that can indicate the presence or absence of particular objects (SIFT). It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game.

In existing system users struggle to set up and maintain privacy settings. 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. In proposed system We are implementing policy recommendation systems which can assist users to easily and properly configure privacy settings.

3. Proposed System

All the Methods that are discussed in the literature survey have some drawbacks. The A3P system i.e Adaptive Privacy Policy Prediction system helps the users to compose privacy settings for their images uploaded on social networking sites. A3P system 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 file information and relationships with others may provide useful information regarding users’ privacy preferences. A3P system consist of two component [1] A3P core and [2] A3P social .When user upload an image ,it will sent to A3P core. A3P core classifies the images based on their content like size, texture and metadata like tags ,comments. Here for the extraction of the features of images we are using SURF instead of using SIFT, which gives us the results within less time .It will decide whether to invoke A3P social. 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.

4. Conclusion

This paper describes various privacy policy techniques for user uploaded data and images in various content sharing sites. The privacy policy can be applied based on the user social behaviour and the user uploaded image content. Future research lead towards improving the performance. To annotate the images, features such as Colour and texture feature are extracted by using Haar wavelet transformation and SURF Descriptors methods. This method will provide more efficient results.

5. References

[1] Anna Cinzia Squicciarini, Member, IEEE, DanLin, Smitha Sundareshwaran, 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


