ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Survey on Secure User Data and Images on Content Sharing Sites implementing APP Scheme and Virtual Password

Priyanka M. Lokhande

Post Graduate Student, Dept. of Information Technology, RMDSSOE Warje, Savitribai Phule Pune University, Pune, India

ABSTRACT: Social networking sites becoming famous day by days. Peoples are uploading images and some personal data on site for that need to provide privacy. The goal of this is to provide a comprehensive review of various privacy policy approaches to improve the security of information shared in the social media sites. An image classification framework for image categories which is correlated with similar policies to automatically produce a policy for each newly updated image, also according to user's social features. To this end, in this paper, provide a virtual password mechanism in which a user can get freedom to select a virtual password scheme which is ranging from weak security to strong security. And also propose a site on which User can share data according to APP, corresponding privacy policy will be implemented on user shared imageto improve the security.

KEYWORDS: Social network, image privacy, content sharing sites, privacy recommendation.

I. INTRODUCTION

The term "social media" refers to the broad range of Internet based and mobile services that allow users to participate in online exchanges, gives user-created content, or join online communities. Online social networks are websites which allow users to build relationships and networks to other Internet users. Information remotely stores by social networks, rather than on a user's personal computer. Social networking can be help to keep in touch with friends, make new contacts and find people with similar interests and views. The relation between a person's social network and privacy is multifaceted. There is a need to develop more security mechanisms for different communication technologies, especially online social networks.

In this paper, mentioned how to prevent user's passwords from being stolen by adversaries in online environments and automated teller machines. We propose differentiated virtual password mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security, where a virtual password requires a small amount of human computing to secure users passwords. The trade-off is that the stronger the scheme, the more complex the scheme may be. Among the schemes, we have a default method, system recommended functions, user-specified functions, user-specified programs, and so on. A function/program is used to implement the virtual password concept with a trade-off of security for complexity requiring a small amount of human computing.

Privacy is necessary to provide security to the design of security mechanisms. Many more social networking sites providers have suggested privacy settings to allow or negate others access to personal information details. Some time in certain occasion's user needs self-information to be known only by a small circle of best friends, and not by hackers or strangers. In other instances, users willing to expose personal information to undescribed strangers, but not to those who know them better. Internet privacy has ability to control what content one reveals about oneself, and who can access that information.

Basically, when the data is collected or recognized without the knowledge or consent of its owner, privacy is desecrated. When it comes to the usage of the data, the owner should be learned about the purposes and intentions for which the data is being or will be used. Most information sharing websites allow users to enter their privacy preferences. One of the main reasons provided is that given the amount of shared information this process can be slow and error-prone.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Therefore, many have acknowledged the need of policy recommendation systems which can support 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.
The privacy of user data can be given by using two methods:
1. User alone can enter the privacy preferences.
2. Recommendation systems assist users for setting the privacy preferences.

The privacy policy of user updated 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 user's privacy preferences. The privacy policy of user uploaded image can be suggested based on the user uploaded image's content and metadata. A hierarchical image classification which classifies images first based on their contents and then refines each category into subcategories 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.

II. RELATED WORK

Anna Cinzia Squicciarini developed an Adaptive Privacy Policy Prediction (A3P) system [1], 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 Meta data information about the images.

Jonathan Anderson proposed a paradigm called Privacy Suites [2] which allows users to easily choose "suites" of privacy settings. A privacy suite can be created by an expert using privacy programming. Privacy Suites could also be created directly through existing configuration UIs or exporting them to the abstract format. The privacy suite is distributed through existing distribution channels to the members of the social sites. The disadvantage is less understandability for end users.

Danezis [3] proposed a machine-learning based approach to automatically extract privacy settings from the social context within which the data is produced.

Adu Oppong **"**Social circles: Tackling privacy in social networks" [4] uses concept of social circles to developed privacy settings. It protects personal information through web based solution. Different technique like Social Circles Finder automatically generates the friend's list. Identify the social circles of the subject, not showing them. Identify social circle of a person, identifies the potency of relationship and so it is providing a significant categorization of friends for setting privacy policies.

Peter F. Klemperer developed a tag based access control of data [5] 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 photo with the participant's friends. The participants can select 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".

Klemperer et al. [6] studied whether the keywords and captions with which users tag their photos can be used to help users more intuitively create and maintain access control policies. Their findings are in line with our approach: tags created for organizational purposes can be repurposed to help create reasonably accurate access-control rules.

Alessandra Mazzia introduced PViz Comprehension Tool [7], an interface and system that corresponds more directly with how users model groups and privacy policies applied to their networks. Such groupings are not always explicit and existing policy comprehension tools which allow 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 distinguish automatically-constructed groups, also address the important sub-

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

problem of producing effective group labels. PViz is better than other current policy comprehension tools Facebook's Audience View and Custom Settings page.

As far as images, J. Yu, D. Joshi, and J. Luo [8] have presented an expressive language for images uploaded in social sites. This work is complementary to ours as we do not deal with policy expressiveness, but rely on common forms policy specification for our predictive algorithm.

Sergej Zerr proposes a technique Privacy-Aware Image Classification and Search [9] to automatically detect private images, and to enable privacy-oriented image search. It combines textual Meta data images with variety of visual features to provide security policies. 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). It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game.

III. METHODOLOGY

The system consists of five main components: Virtual password, Access privacy policy, Access policy prediction, Social media and Image encryption.An Access Privacy Policy system that helps users automates the privacy policy settings for their uploaded images. The APP system provides a comprehensive framework to infer privacy preferences based on the information available for a given user.

An Access Privacy Policy system using color Scheme authentication which aims to provide users a hassle free privacy settings experience by automatically generating personalized policies. A policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to user's social features.

The overall data flow is the following. When a user uploads an image, the image will be first sent to the APP. The APP separates the image and determines whether there is a need to provoke the social media. In most cases, the APP predicts policies for the users directly based on their historical behaviour. If one of the following two cases is verified true, APP will invoke Social Media: (a) The user does not have enough data for the type of the uploaded image to conduct policy prediction; (b) The APP detects the recent major changes among the user's community about their privacy practices along with user's increase of social networking activities.

APP is Access Privacy Policy which defines the source access policy for user shared data and images. This policy will be getting implemented on shared contents according to contents and to whom it will be shared. There is a major component in APP i.e. Image classification. For each user, images are first classified based on content and metadata. Groups of images that may be associated with similar privacy preferences, in the proposed System, a hierarchical image classification which classifies images first based on their contents and then refine each category into subcategories 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.

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. The prediction process consists of two main phases: (a) policy mining; and (b) policy prediction.

(a)**Policy mining:** Privacy Policies are the privacy preferences expressed by the user. Policy mining deals with mining of these policies by applying different association rules and steps. This approach starts by looking the popular actions in the policies containing the popular subjects in policies and finally for conditions.

(b)**Policy prediction:** The policy Prediction is used to choose the best policy for the user by obtaining the strictness level. The strictness level decides how strict a policy is by returning an integer value. This value should be minimum to attain high strictness. The strictness can be discovered by two matrices: a major level and coverage rate.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

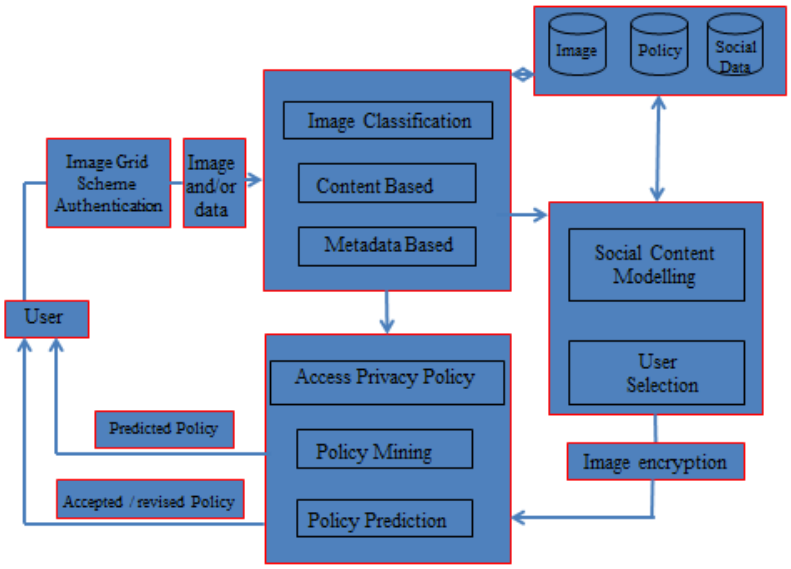

Fig.1. Framework of System Architecture.

In above cases, it would be useful to report to the user the latest privacy practice of social communities that have similar background as the user. The social media groups users into social communities with similar social context and privacy preferences, and continuously monitors the social groups. When the social media is invoked, it automatically identifies the social group for the user and sends back the information about the group to the APP for policy prediction. At the end, the predicted policy will be displayed to the user. 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.

The social media 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, social media will be invoked by the APP-in two scenarios. One is when the user is a newbie of a site, and does not have enough images stored for the APP to infer meaningful and customized policies. The social content modelling 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 that have similar content and privacy preferences.

Access Privacy Policy (APP) system, a free privacy settings system by automatically generating personalized policies. The APP system handles user uploaded images based on the person's personal characteristics and images content and metadata. Users can even give same value for two different colours. This makes the authentication method risk free of shoulder attack, dictionary attack, eves dropping etc.

IV. CONCLUSION

Proposed system concludes privacy policy techniques for user uploaded data images in various content sharing sites. Based on the user social behaviour and the user uploaded image, the privacy policy can applied. APP system in used, which provide users easy and properly, configured privacy setting for their uploaded image. By using this can easily prevent unwanted discloser and privacy violations. Unwanted disclosure may lead to misuse of one's personal information. Users automate the privacy policy settings for their uploaded images with the help of access privacy policy (APP). Based on the information available for a given user the APP system provides a comprehensive framework to infer privacy preferences.

Thus proposed a system having a new perspective on content sharing in social sites to improve the security of information shared in the social media sites. Using all this content and above methods privacy recommendation can be easier.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

V. ACKNOWLEDGMENT

I would like to express my gratitude towards Ms. Pratibha Chavan for her persistence guidance throughout the project. I would like to thank Mr D. A. Meshram for their constructive criticism and Mrs Sweta Kale for their valuable support.

REFERENCES

1. 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.
2. J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.
3. J. Bonneau, J. Anderson, and G. Danezis, "Prying data out of a social network," in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining. , pp.249–254,2009.
4. 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.
5. 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., pp. 377–386, 2012.
6. K. Lerman, A. Plangprasopchok, and C. Wong, "Personalizing image search results on flickr," CoRR, vol. abs/0704.1676, 2007.
7. A. Mazzia, K. LeFevre, and A. E."The PViz comprehension tool for social network privacy settings," in Proc. Symp. Usable Privacy Security, 2012.
8. 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, pp.1464–1467, 2009.
9. S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, "Privacy-aware image classification and search," in Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inform. Retrieval, pp. 35–44, 2012.