A Powerful Technique for Maintaining Privacy of Images on Content Sharing Sites

Prof. Uttam R. Patole[1], Neha L. Jain[2], Tejasvini S. Baviskar[3], Gauri A. Bhosale[4], Sneha M. Chaudhari[5]

[1]*Assistant Professor, Computer Department, S.V.I.T, Chincholi, Nasik, Maharashtra, India*
[2345]*B.E Student, Computer Department, S.V.I.T, Chincholi, Nasik, Maharashtra, India.*

ABSTRACT

Now days the amount of sharing images on the content sharing sites has increased, so maintaining the privacy has become a major problem area. In sight of these incidents, the need to seek the tools to help users control the access to their shared contents is apparent. Towards addressing this needs we proposed an Adaptive Privacy Policy Prediction (A3P) system. This system will help user to compose the privacy settings for their images .Here a two level framework is used, which according to the users available history on the site, determines the best available privacy policy for the users image which are to be uploaded on the site. Our framework for image categories which may be associated with similar policies. We examine the role of social context, image context and metadata as the possible indicators of users privacy policy for the users image being uploaded. We also have tried to efficiently tackle the problem of unnecessary and useless comments. The comments on a particular photo can be blocked if it contains any bad words or any such words which may harm the users social image on the social networking sites. Our goal is to improve the set of privacy controls and defaults, but we are limited by the fact that there has been no in-depth study of users privacy settings on sites like Facebook. While significant privacy violations and mismatched user expectations are likely to exist, the extent to which such privacy violations occur has yet to be quantified. Images are now one of the key enablers of users connectivity.

Keyword: - *A3P (Adaptive Privacy Policy Prediction), CSS (Content Sharing Sites), OSN (Online Social Network).*

1. INTRODUCTION

The sharing of personal data has emerged as a popular activity over online social networking sites like Facebook. As a result, the issue of online social network privacy has received significant attention in both the research literature and the mainstream media. Our overarching goal is to improve defaults and provide better tools for managing privacy, but we are limited by the fact that the full extent of the privacy problem remains unknown; there is little quantization of the incidence of incorrect privacy settings or the difficulty users face when managing their privacy. With the increasing volume of images users share through social sites, maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need, we propose an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. We propose a two-level framework which according to the users available history on the site, determines the best available privacy policy for the users images being uploaded. Our solution relies on an image classification framework for image categories which may be associated with similar policies, and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to user's social features.

We focus on measuring the disparity between the desired and actual privacy settings, quantifying the magnitude of the problem of managing privacy. We deploy a survey, implemented as a Facebook application, to 200 Facebook users recruited via Amazon Mechanical Turk. We and that 36 percent of content remains shared with the default privacy settings. We also and that, overall, privacy settings match users expectations only 37 percent of the time, and when incorrect, almost always expose content to more users than expected. Finally, we explore how our

results have potential to assist users in selecting appropriate privacy settings by examining the user-created friend lists. We and that these have significant correlation with the social network, suggesting that information from the social network may be helpful in implementing new tools for managing privacy. 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 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. Some users over CSS affects users privacy on their personal contents, where some users keep on sending unwanted comments and messages by taking advantage of the users inherent trust in their relationship network. By this privacy of the user data may be loss for this issue this paper handles the most prevalent issues and threats targeting different CSS recently. This proposes a privacy policy prediction and access restrictions along with blocking scheme for social sites using data mining techniques.

2. LITERATURE SURVEY

Social networking can be used to keep in touch with friends, make new contacts and find people with similar interests and ideas. The relation between privacy and a person's social network is multi-faceted. There is a need to develop more security mechanisms for different communication technologies, particularly online social networks. Privacy is essential to the design of security mechanisms. Most social networks providers have offered privacy settings to allow or deny others access to personal information details. In certain occasions we want information about ourselves to be known only by a small circle of close friends, and not by strangers. In other instances, we are willing to reveal personal information to anonymous strangers, but not to those who know us better. Social network theorists have discussed the relevance of relations of different depth and strength in a person's social network and the importance of so-called weak ties in the flow of information across different nodes in a network. Online social-networking services, which allow users to label other users as "friends", thereby sharing with them a wide variety of personal information ranging from favorite movies to resumes, have become incredibly popular. Facebook, for example, has over 70 million active users. As social networks have grown in size, and as the term "friend" has become all-encompassing, it has become increasingly difficult for users to control which friends get to see what personal information. Despite the privacy controls available on such social-networking services, many users neglect to control their privacy because it is difficult to set privacy policies. Also, a study shows that college students rarely utilize the different privacy settings on Facebook and are often unaware of their own privacy settings. A tag based access control of data is developed by Peter F. Klemperer. It is a system that creates access-control policies from photo management tags.

3. PROPOSED 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. At the most basic level, an online social network is an Internet community where individuals interact, often through profiles that (re)present their public persona (and their networks of connections) to others. Although the concept of computer-based communities dates back to the early days of computer networks, only after the advent of the commercial Internet did such communities meet public success? Following the SixDegrees.com experience in 1997, hundreds of social networks spurred online (see [4] for an extended discussion), sometimes growing very rapidly, thereby attracting the attention of both media and academia. In particular, [5], [6], and [7] have taken the no graphic and sociological approaches to the study of online self-representation; [8] have focused on the value of online social networks as recommender systems; [4] have discussed information sharing and privacy on online social networks, using FB as a case study; [9] have demonstrated how information revealed in social networks can be exploited for "social" phishing; [10] has studied identity-sharing behavior in online social networks.

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. Ownership is an important issue in photos for online social networks, as many users upload photos of other people. We questioned the social acceptance of modifying or deleting photos that perhaps seem to belong to other people. Even before we asked direct questions about ownership, participants naturally brought it up regarding their

general concerns and problems of photo sharing. In proposed System an Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. We also effectively tackled the issue of cold start, leveraging social context information. Our experimental study proves that our A3P is a practical tool that offers significant improvements over current approaches to privacy. 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 too 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.

4. SYSTEM ARCHITECTURE

The proposed A3P system is comprised of two main building blocks: A3PSocial and A3P-Core. The A3P-core focuses on analyzing each individual users 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.

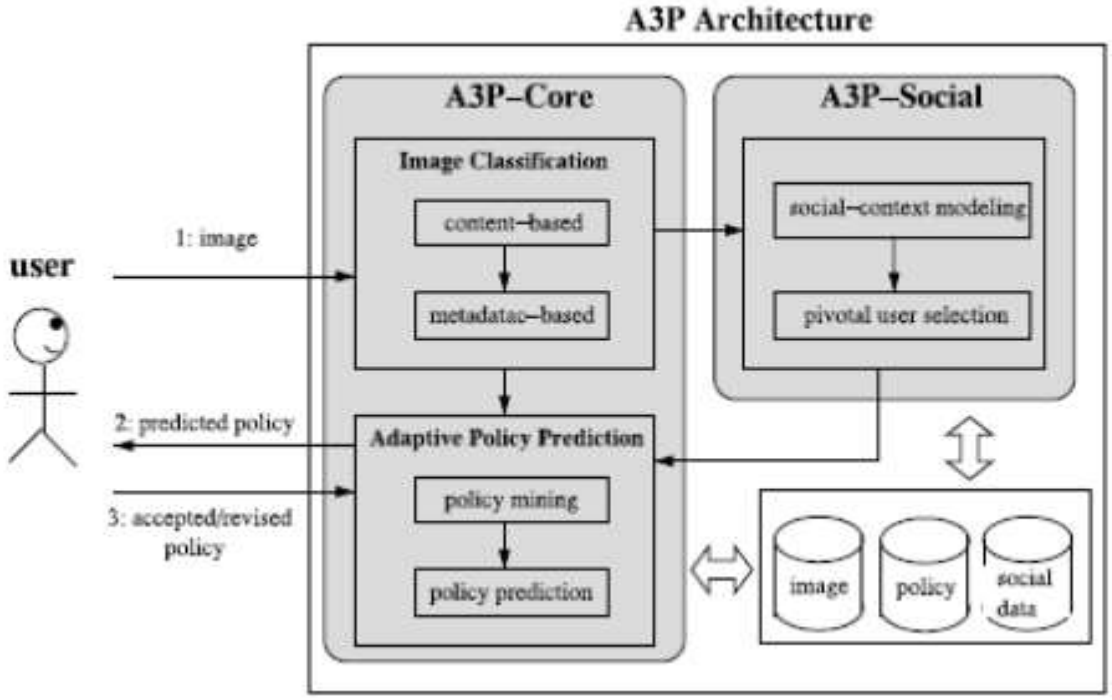

Fig-4.1: System Architecture

The A3P system consists of two main components: A3P-core and A3P-social. The overall data flow is the following. 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. In most cases, the A3P-core predicts policies for the users directly based on their historical behavior. If one of the following two cases is verified true, A3P-core will invoke A3Psocial: (i) The user does not have enough data for the type of the uploaded image to conduct policy prediction; (ii) The A3P-core detects the recent major changes among the users community about their privacy practices along with users increase of social networking activities (addition of new friends, new posts on ones profile, etc.). The A3P-social groups users into social communities with similar social context and privacy preferences, and continuously monitors the social groups. When the A3Psocial is invoked, it automatically identifies

the social group for the user and sends back the information about the group to the A3P-core 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 actual policy will be stored in the policy repository of the system for the policy prediction of future uploads.

5. ALGORITHM

5.1 ALGORITHM FOR CREATE AN ACCOUNT FOR USER:

1. Start.
2. If already account created then sign in else go to next step.
4. Display account information Details like Name, Address, Email, Mobile Number, Gender, City and Password.
5. If all details are filled and Email-id is valid then user gets UserID via Email else go to previous step.
6. Otherwise create account.
7. Login.
8. Stop.

5.2 ALGORITHM FOR WORKING OF SYSTEM:

1. Start.
2. After login the page will be open and profile visible to user.
3. Create album.
4. Upload image.
5. Display the image which is uploaded on user profile.
6. Add Friends and manage labels to the friend.
7. Post comment.
8. Block comment if it uses violent word.
9. Change password if required.
10. Logout.
11. Stop.

6. SNAPSHOTS

Fig-6.1: User Registration

Fig-6.2: Account Information

Fig-6.3: Create Album

Fig-6.4: Upload Image

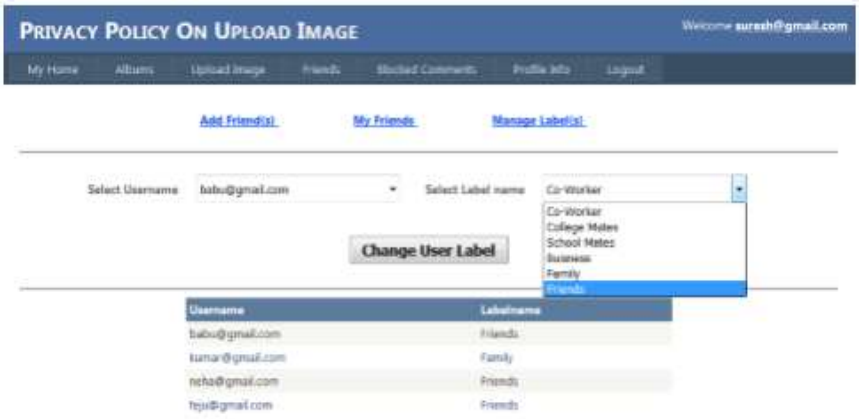

Fig-6.5: Manage Labels

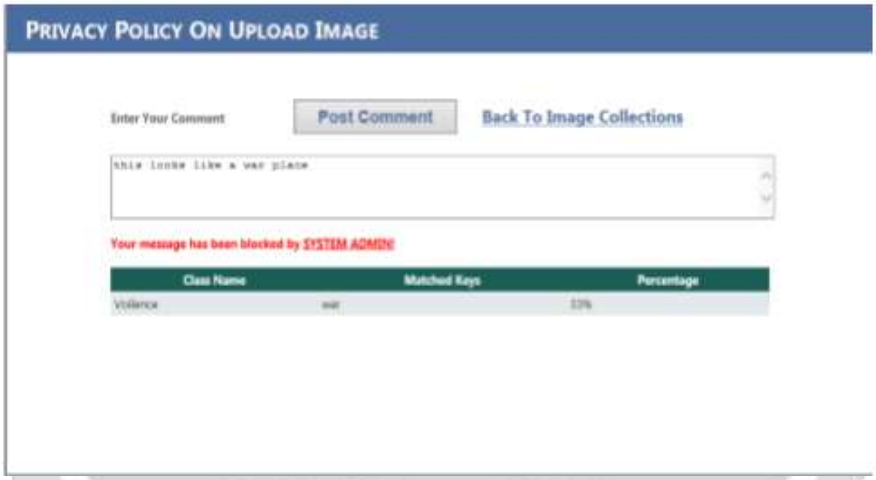

Fig-6.6: Post Comment

Fig-6.7: Block List

7. CONCLUSION

We have proposed an Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. We also effectively tackled the issue of cold start, leveraging social context information. Our experimental study proves that our A3P is a practical tool that offers significant improvements over current approaches to privacy.

8. ACKNOWLEDGEMENT

We take this opportunity to express our hearty thanks to all those who helped us in the completion of the project. We express our deep sense of gratitude to our internal guide Prof. U. R. Patole, Asst. Prof., Computer Engineering Department, Sir Visvesvaraya Institute of Technology, Chincholi for their guidance and continuous motivation. We gratefully acknowledge the help provided by them on many occasions, for improvement of this project with great interest. We would be failing in our duties, if we do not express our deep sense of gratitude to Prof. S. M. Rokade, Head, Computer Engineering Department for permitting us to avail the facility and constant encouragement. We would also like to thank Prof. R. B. Bhosale Project Co-ordinator for his great support and excellent guidance. We express our heartiest thanks to our known and unknown well-wishers for their unreserved cooperation, encouragement and suggestions during the course of this project report. Last but not the least, we would like to thanks to all our teachers, and all our friends who helped us with the ever daunting task of gathering information for the project.

9. 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 DataBases, 1994, pp. 487-499.

[3] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "Overexposed?: 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. 971980.

[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] 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.

[7] 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.

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

[9] 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., 2012, pp. 377-386.

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

[11] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in Proc. ACM SIGCOMM Conf. Internet Meas. Conf., 2011, pp. 61-70.

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

[13] A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, "A3p:Adaptive policy prediction for shared images over popular content sharing sites," in Proc. 22nd ACM Conf. Hypertext Hypermedia,2011, pp.261-270.

[14] K. Lerman, A. Plangprasopchok, and C. Wong, "Personalizing image search results on flickr," CoRR, vol. abs/0704.1676, 2007.

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

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