ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Providing P3 Approach to Improve Security over Social Media

Mandadapu Spandana
M.Tech,
Dept of CSE,
Swarna Bharathi College of Engineering,
Khammam.

Mr.Mudusu Ram Babu, M.Tech
Associate Professor & HOD,
Dept of CSE,
Swarna Bharathi College of Engineering,
Khammam.

Abstract:
Now a day's sharing data and images on social networking sites must and should maintain privacy and security. We proposed a method P3 privacy policy prediction system to helps users from lack of security and privacy of sharing data and images on social sites. User's available history on the site, determines the best available privacy policy for the user's images being uploaded. a privacy policy predication and access restrictions along with blocking the particular sites on network using some techniques. The Framework determines the best privacy policy for the uploaded images. It includes an Image classification framework for association of images with similar policies and a policy prediction technique to automatically generate a privacy policy for user-uploaded images. The system utilizes APP access policy predication (APP). 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.

Keywords: P3, APP, Security, SN, SM.

1. Introduction:
Sharing data over social sites become a key point of users. The sharing takes place both group of people or social circles that include google+, facebook, orkut, whatapp. users of social media can define a personal information and that may edit by this features allows by the SM(Social Media).a method was proposed to provide in SN(Social Network) is to produce proposition for finding new groups, relations and finding new people and events using techniques. Social media sites are used by huge number of users around the world. it provides different features to the customers like chatting and adding comments to an images, sharing images, downloading content, movies. To prevent such kind of unwanted disclosure of personal images, flexible privacy settings are required.

In recent years, such privacy settings are made available but setting up and maintaining these measures is a tedious and error prone process. Therefore, recommendation system is required which provide user with a flexible assistance for configuring privacy settings in much easier way. In this paper, we are implementing a Privacy Policy Prediction (P3) system which will provide users a hassle free privacy settings experience by automatically generating personalized policies.

2. Literature Survey:
Some older versions show different studies on automatically assign the privacy settings. the privacy sites used by expert users are trusted friends who already set the settings for the users. Based on concepts of social circles by forming clusters of friends the study of whether the keywords used for editing user images can be used more efficiently to create and access control polices.

3. System Architecture:

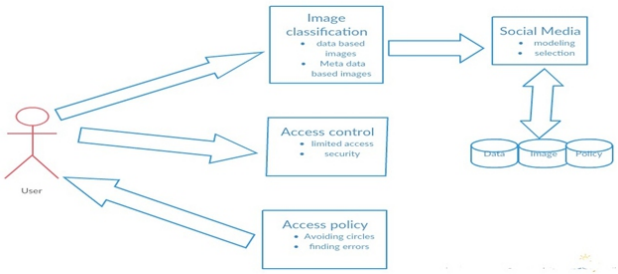

Figure 3.0 shows System Architecture

3.1 System Overview:
The P3-social groups users into social communities with similar social context and privacy preferences, and continuously monitors the social groups. When the P3-social is invoked, it automatically identifies the social group for the user and sends back the information about the group to the P3-core for policy prediction.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

3.2. P3 Architecture:

P3 stands for Adaptive Privacy Policy Prediction system which helps users to derive the privacy settings for their images The P3 Architecture consists of followings blocks:

1. Image classification.
2. Access Control
3. Access Policies

The Access Privacy Policy looks if the image or similar type of image already exists which can be given with similar privacy policies. If similar type of image doesn't exist then it looks for all the policies and lets user choose the policies.

3.3 Access Policy:

Access policy is for retrieving the data or image in the network. By this kind of right of entry privacy may loss. For this problem the user of the social media compute the normalized and prejudiced average of the ratings of the users in the district. User have to confine the neighbor circle so un-wanted may not influence the data. When it comes to the usage of the data, the owner should be knowledgeable about the principle and purpose for which the data is organism or will be used and to provide a partiality.

3.4 Access control:

Access control in the shared environment is one of the essential one. To supply a secure access we have to limit the unauthorized user in these networks. Access control mechanism (ACM) is one of the privacy conserve one.

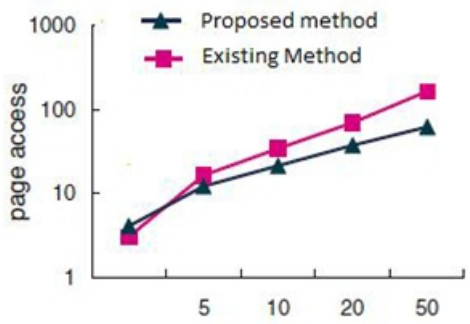

Figure 3.4 shows diverse between existing and the proposed system

These shows the diverse between existing and the proposed system (see figure 3.4). In the proposed system the access of the pages were limited when compared to existing system. Access control is by provided that access rights in a SN are limited to few basic constitutional rights, such as read, write and play for media content. This based type of approach which generates access-control policies from photo administration tags. Every photo is integrated with an access grid for mapping the photo with the participant's friends. The contestant can select a suitable partiality and access the information. Photo tags can be categorized as directorial or forthcoming based on the user needs.

3.5 P3 Social:

In the second round of experiments, we analyze the performance of the P3-Social component using the first set of data collection. For each user, we use the P3-Social to predict policies and compare it with three other alternative approaches :(i) prediction based on only similarity of privacy strictness levels; (ii) prediction based on Cosine similarity; (iii) prediction based on Pearson. In particular, the first base-line approach does not consider social contexts but bases recommendation only on social groups that have similar privacy strictness level for same type of images. The second approach adopts Cosine similarity to measure the similarity of the social contexts between the new user and all the existing users, and then finds the top two users with the highest similarity score as the candidate users. The images of the candidate users are then sent to the P3 is for the policy predication.

Social Context:

We observe that users with similar background tend to have similar privacy concerns, as seen in previous research studies and also confirmed by our collected data. This observation inspires us to develop a social context modeling algorithm that can capture the common social elements of users and identify communities formed by the users with similar privacy concerns.Formally, we model the ratio of each type of relationship among all contacts of a user as social connection. Let R1... Rn denotes the n types of relationships observed among all users. Let NuRi denote the number of user U's contacts belonging to relationship type Ri. The connection distribution (denoted as Conn) is represented as below:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

$$Conn : \{\frac{N^u_{R_1}}{\sum_{i=1}^{n} N^u_{R_i}}, \ldots, \frac{N^u_{R_n}}{\sum_{i=1}^{n} N^u_{R_n}}\}.$$

For example, suppose that there are four types of relationships being used by users in the system: R1="family", R2="colleague", R3="friend", R4="others". Bob has 20 contacts, among which he has 10 family members, 5 colleagues, and 5 friends. His social connection is represented as
{10/20, 5/ 20, 5/ 20, 0/ 20}.

Social Group:

We now introduce the policy recommendation process based on the social groups obtained from the previous step. Suppose that a user U uploaded a new image and the A3P-core invoked the P3-social for policy recommendation. The P3-social will find the social group which is most similar to user U and then choose the representative user in the social group along with his images to be sent to the P3 policy prediction module to generate the recommended policy for user U. Given that the number of users in social network may be huge and that users may join a large number of social groups, it would be very time consuming to compare the new user's social context attributes against the frequent pattern of each social group.

4. CONCLUSION:

We have proposed a Privacy Policy Prediction (P3) system that helps users automate the privacy policy settings for their uploaded images. The P3 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 P3 is a practical tool that offers significant improvements over current approaches to privacy. Social network is an upgrading media for information sharing through internet. It provides a content sharing like text, image, audio, video, etc… With this emerging E-service for content sharing in social sites privacy is important issue. These provide a privacy policy prediction and access restrictions along with blocking scheme for social sites and improve the privacy level for the user in social media. This system provides a framework which deduces privacy preference based on the history of the users proclivity. This help user to set hassle free and flexible policy selection.

5. 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]. S.Thiraviya Regina Rajam1 and Dr. S.Britto. Ramesh Kumar, "SOCIAL NETWORK SERVICES: ANOVERVIEW".

[3] H. Sundaram, L. Xie, M. De Choudhury, Y. Lin, and A. Natsev,"Multimedia semantics: Interactions between content andcommunity," Proc. IEEE, vol. 100, no. 9, pp. 2737–2758, Sep. 2012.

[4] S. Ahern, D. Eckles, N. Good, S. King, M. Naaman, and R. Nair. Over-Exposed? Privacy Patterns and Considerations in Online and Mobile Photo Sharing.CHI, 2007.

[5] Sangeetha. J, Kavitha. R, "An Improved Privacy Policy Inference over the Socially Shared Images with Automated Annotation Process"

[6]. 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.

[7]. 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.

[8] R. Datta, D. Joshi, J. Li, and J. Wang. Image retrieval: Ideas, influences, and trends of the new age. ACM Computing Surveys (CSUR), 40(2):5, 2008.

[9] J. Deng, A. C. Berg, K. Li, and L. Fei-Fei. What does classifying more than 10,000 image categories tell us? In 11th European conference on Computer vision: Part V, ECCV'10, Berlin, Heidelberg, 2010. Springer-Verlag.

[10] A. K. Fabeah Adu-Oppong, Casey Gardiner and P. Tsang. Social circles: Tackling privacy in social networks. In Symposium on Usable Privacy and Security, 2008.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[11] L. Geng and H. J. Hamilton. Interestingness measures for data mining: A survey. ACM Comput. Surv, 38(3):9, 2006.

[12] Image-net Dataset. www.image-net.org.

[13] S. Jones and E. O'Neill. Contextual dynamics of group based sharing decisions. In Conference on Human Factors in Computing Systems, CHI '11, pages 1777–1786. ACM, 2011.

[14] 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

[15] 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.

[16] 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.

[17] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable Privacy Security, 2009.
Harsh A Patel et al, Int.J.Computer Technology & Applications, Vol 6 (5), 835-838 IJCTA |

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

[19] 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!: Usingtags for access control in photo sharing," in Proc. ACM Annu.Conf. Human Factors Comput. Syst., 2012, pp. 377–386.

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