Providing Security from various attacks and Preserving Privacy in Online Photo Sharing Mechanism

Vennela.A#1, Nagaraju.J#2, Syamsundar.T#3,
Sriharshavardhan.B#4, Srikanth.N#5, Prudhvi.M#6

#1 Assistant professor, Dept Of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)
#2 Student, Dept Of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)
#Student, Dept Of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)
#4 Student, Dept Of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)
#5 Student, Dept Of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)
#6 Student, Dept Of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)

Abstract:Online social networks have now become the most popular platforms for people to share information with others. Along with this, there is a serious threat to individuals' privacy. In the proposed system, a trust-based mechanism to realize collaborative privacy management. Basically, a user decides whether or not to post a data item based on the aggregated opinion of all involved users. The trust values between users are used to weight users' opinions, and the values are updated according to users' privacy loss. Moreover, the user can make a trade-off between data sharing and privacy preserving by tuning the parameter of the proposed mechanism. If any of the hacker hack the database of the user, the information or photos that are shared between the users are get hacked. To provide the better security for the database, Secured Hash Algorithm is introduced and it avoids the hacking of password in the database. The proposed system mainly focuses on the privacy management on photo sharing and password protection. It plays the two-level protection on the social networks

Keywords:social trust, voting scheme, multi-armed bandit, collaborative privacy management, online social network.

I. INTRODUCTION

It's obvious that people are more likely to use online social networks such as Google+, Twitter and Facebook for their needs to connect with the society. It has become common for people to upload and post information about the daily events in text, photos and video format in these types of social network sites. Such posts may involve sensational information [1] of the user who posted the data or of other persons. In case, the data is exposed to some unofficial persons, security of the user's data will be on risk. Privacy problem is one of the major points of study concerning the usage of social network sites.It's a great responsibility of the service providers of these sites to form methods for protecting the uses data from being hacked. Meanwhile the users [2], [3] also can decide their own data access by making use of the privacy setting facilities provided by the social network sites. The level of privacy of the person using a social network site will be clearly explained by the particular site including the information of whom can access the data and this

information's are collectively named as privacy policy. The information of the relationship between users has been made used by the online social networks to find the difference between official and unofficial users.The power of a Facebook user to determine the exposure of his or her data to friend for particular groups or everyone is a great example of improved authority over the accessibility of the data.These privacy measures taken by recent online social networks apply restriction only on the users who need to access other user's data. Despite, there is no governance over the users who upload the particular data. This may lead to the users posting data and breaking the privacy policy rules without any motive. For example, consider a person A uploading a photo of himself dancing with person B. Here, person A has posted the photo consciously. But, it is not sure that person be has full will on posting the particular photo. So, the privacy of person B is in risk as the post is out of B's consciousness. Here the person A unintentionally violates the privacy policy of the online social network and person B suffers privacy issue. Complication is that the picture which is posted is co-owned by both A and B. In online social networks it is common for two or more persons owning same photo. Maintaining privacy [4]policy needs a good cooperation between multiple users of same post.

Managing the cooperation between the users has become a challenge for online social networks. First the problems arising in the privacy of the users must be studied well and then corrected policies should be generated by the OSN. Privacy policy basically interconnects the user who uses the data and all other users to whom the owner wants the data to share with. A middle person involves in gathering all the user"s policy and making a collective determination through an aggregation scheme [5]-[7]. These developed privacy schemes do not always assure cent percent privacy to the users, hence the conflict will still exist. The method that can be used for eliminating the conflict between data sharing and privacy protection is being the most important questions among online social networks.

In traditional methods a mediator lies between the user who posts data and the users who are involved in the post to make an effective collaboration between the users. But in this approach the posting user itself is directly in collaboration with the users who are involved in the post tense should assure that the privacy is met. The past system consists of facilities where the user can upload a photo in which all the users involved are tagged in or they can be easily found out by some other recognizing techniques [8]. Here as the mediator is in between he also comes to know the uses involved in the particular post. Practically it is impossible or hard to identify or recognize the users involved in the post automatically. Hence we propose a system in which the user who posts the data is supposed to get permission from all the users that are involved in the post. This may be considered as such trust-weighted voting scheme.

Particularly whenever a data or information is to be posted by a user he or she gets a vote from all the involved users which are an approval for whether the data is to be posted and the post is inclusive of all involved user's privacy policy. The trust value lying between the user who post the data and the user who is involved in the post determines the importance of the voting system [9]. The

time the data gets fulfilled of all permission through the voting system the particular data gets approved to be posted. Here, the trust value can be altered and it is not fixed. A user's trust on other one gets lost if the other user posts data that affects the privacy of the first person. Likewise, user wants more trust if he or she follows and prospects the opinions of others. Now, it gets total responsibility for the user to lose or gain their trust value, thus he or she becomes alert while posting data thereby securing the privacy of the user involved.

II. RELATED WORK

Over-Exposed? Privacy Patterns and Considerations in Online and Mobile Photo Sharing

As sharing personal media online becomes easier and widely spread, new privacy concerns emerge – especially when the persistent nature of the media and associated context reveals details about the physical and social context in which the media items were created. In a first-of-its-kind study, we use context-aware camera phone devices to examine privacy decisions in mobile and online photo sharing [10]. Through data analysis on a corpus of privacy decisions and associated context data from a real-world system, we identify relationships between location of photo capture and photo privacy settings. Our data analysis leads to further questions which we investigate through a set of interviews with 15 users. The interviews reveal common themes in privacy considerations: security, social disclosure, identity and convenience. Finally, we highlight several implications and opportunities for design of media sharing applications, including using past privacy patterns to prevent oversights and errors.

Privacy Suites: Shared Privacy for Social Networks

Creating privacy controls for social networks that are both expressive and usable is a major challenge. Lack of user un-derstanding of privacy settings can lead to unwanted disclosure of private information and, in some cases, to material harm. We propose a new paradigm which allows users to easily choose \suites" of privacy settings [11] which have been specified by friends or trusted experts, only modifying them if they wish. Given that most users currently stick with their default, operator-chosen settings, such a system could dramatically increase the privacy protection that most users experience with minimal time investment.

SheepDog – Group and Tag Recommendation for Flickr Photos by Automatic Search-based Learning

Online photo albums have been prevalent in recent years and have resulted in more and more applications developed to provide convenient functionalities for photo sharing. In this paper, we propose a system named *SheepDog*to automatically add photos into appropriate groups and recommend suitable tags for users on Flickr. We adopt concept detection to predict relevant concepts of a photo and probe into the issue about training data collection for concept classification. From the perspective of gathering training data by web searching, we introduce two mechanisms and investigate their performances of concept detection [12]. Based on some existing information from

Flickr, a ranking-based method is applied not only to obtain reliable training data, but also to provide reasonable group/tag recommendations for input photos. We evaluate this system with a rich set of photos and the results demonstrate the effectiveness of our work.

Personalizing Image Search Results on Flickr

The social media site Flickr allows users to upload their photos, annotate them with tags, submit them to groups, and also to form social networks by adding other users as contacts. Flickr offers multiple ways of browsing or searching it. One option is tag search, which returns all images tagged with a specific keyword. If the keyword is ambiguous, e.g., "beetle" could mean an insect or a car, tag search results will include many images that are not relevant to the sense the user had in mind when executing the query. We claim that users express their photography interests through the metadata they add in the form of contacts and image annotations. We show how to exploit this metadata to personalize search results for the user, thereby improving search performance [13], [14]. First, we show that we can significantly improve search precision by filteringtag search results by user's contacts or a larger social network that includes those contact's contacts. Secondly, we describe a probabilistic model that takes advantage of tag information to discover latent topics contained in the search results. The users' interests can similarly be described by the tags they used for annotating their images [15]. The latent topics found by the model are then used to personalize search results by finding images on topics that are of interest to the user.

III METHODOLOGY

Online Social Network

An OSN can be characterized by an edge-labeled directed graph G = (V, E), where V is the set of vertices and E is the set of edges. Every single vertex signifies a user. In subsequent descriptions, unless otherwise specified, we promote the two terms "vertex" and "user" manageable. Every single edge in the graph denotes a correlation between two users. Let RT stand for the set of relationship types hold up by the OSN. The edge from user"s v_i to v_j can be shown by a 3-tuple (v_i, v_j, r_{ij}), where r_{ij} 2 RT is the label associated with the edge. By swapping all the directed edges in G with undirected edges, we can manage the distance between any two users. Specifically, given a pair of users (v_i, v_j), if there is a route between the two users, then the distance d_{ij} is definite as the length of the shortest path between user"s v_i and v_j. If there is no path between user"s v_i and v_j then we define d_{ij} = 1. For example, in the graph showed in Fig. 1, the distance between two users a and c is 1, and the distance between a and g is 3.

Trust Evaluation

Trust plays a crucial role in the privacy managing mechanism anticipated in this paper. For any two user"s v_i and v_j, no matter they are directly coupled by an edge or not, we use t_{ij} to signify the trust of user v_i in user v_j. We define t_{ij} 2 [0; 1]. The more usersvi trusts user v_j, the higher t_{ij} is.The trust of user v_j in user vi is denoted as v_{ji}. Generally, thereis v_{ij} 6= v_{ji}. Various models have been

proposed to evaluatetrust in social networks, including network structurebasedmodels [13] and interaction-based models [14]. In thispaper, we mainly focus on how the trust between users canbe leveraged to realize collective privacy management. Herewe first use a simple distance-based method to determinethe initial trust values. And in the following section, we willdiscuss how to update the trust values based on the interactionsbetween users.Given a pair of users vi and v_j , we define t_{ij} = 0 if d_{ij} =1. If the two users are directly connected, namely d_{ij} = 1,t_{ij} is set to a positive constant which is determined by therelationship type r_{ij} . For example, if user v_j is user v_i"s familymember, we can set t_{ij} = 0:8; while if user vj is user vi"scolleague, we can set t_{ij} to a lower value, say 0:6. When1 <d_{ij}< 1, we utilize the transitivity property of trust [15],[16] to compute the trust value. Specifically, t_{ij} is computedbyt_{ij}.

Given a pair of user"sv_i and v_j, we define t_{ij} = 0 if d_{ij}=1. If the two users are directly connected, namely dij = 1,t_{ij} is set to a positive constant which is determined by the relationship type r_{ij} . For example, if user v_j is user v_i"s family member, we can set t_{ij} = 0:8; while if user v_j is user vi"s colleague, we can set t_{ij} to a lower value, say 0:6. When 1 <d_{ij}< 1, we utilize the transitivity property of trust to compute the trust value. Specifically, t_{ij} is computed by

$$t_{ij}=\pi_{k=1},\ldots..,d_{ij}t_{pk}\ p_{k+1},$$
$$(v_{pk},v_{pk+1})\text{€}Path\ _{ij}$$

Multiparty Access Control

An eminent characteristic of OSNs is that they afford expedient ways for users to share data with others. Usually, a user can: post a data item, such as a photo, a video clip or a text message, in his/her own space or additional user"s space; distribute a data item, which was formerly posted by alternative user, by sending it in his/her own space.In either one of the overhead two cases, we denote to the user as the owner of the data item. Properly, given a data item d, we signify the owner of d as od. If d encompasses multiple users, then d is co-owned by the users. All the users related with d, except od, areindicated to as consumers.

IV ARCHITECTURE

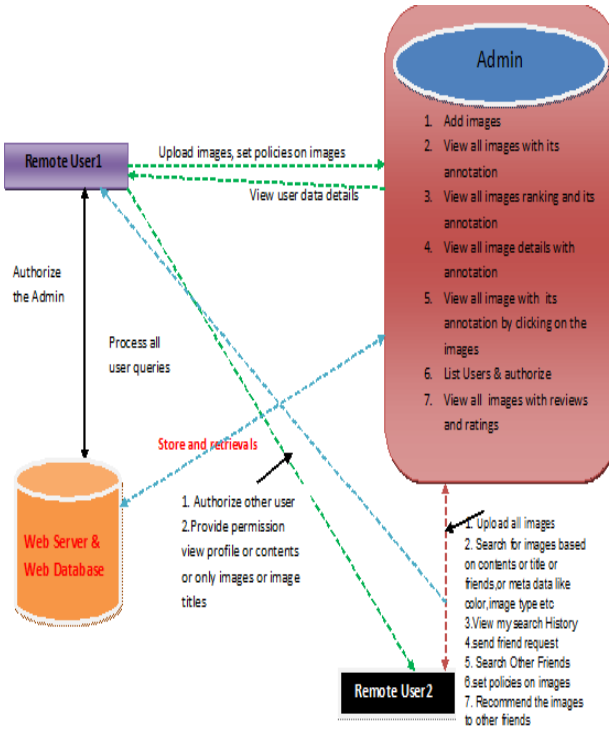

Fig System Structure

COMPONENTS

System Construction Module

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 user's community about their privacy practices along with user's increase of social networking activities (addition of new friends, new posts on one's profile etc).

Content-Based Classification

To obtain groups of images that may be associated with similar privacy preferences, we propose 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. Note that it is possible that some images are included in multiple categories as long as they contain the typical content features or metadata of those categories.

Our approach to content-based classification is based on an efficient and yet accurate image similarity approach. Specifically, our classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. For each image, the wavelet transform encodes frequency and spatial information related to image color, size, invariant transform, shape, texture, symmetry, etc. Then, a small number of coefficients are selected to form the signature of the image. The content similarity among images is then determined by the distance among their image signatures.

Metadata-Based Classification

The metadata-based classification groups images into subcategories under aforementioned baseline categories. The process consists of three main steps. The first step is to extract keywords from the metadata associated with an image. The metadata considered in our work are tags, captions, and comments. The second step is to derive a representative hypernym (denoted as h) from each metadata vector. The third step is to find a subcategory that an image belongs to. This is an incremental procedure. At the beginning, the first image forms a subcategory as itself and the representative hypernyms of the image becomes the subcategory's representative hypernyms.

Adaptive Policy Prediction

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 three main phases: (i) policy normalization; (ii) policy mining; and (iii) policy prediction.

V CONCLUSION

In this paper we study the privacy issue caused by the distribution of co-owned information in OSNs. To help the owner of data cooperate with the consumers on the control of data sharing, we recommend a trust-based mechanism. When a consumer is about to post a data item, the user first implores the consumers‟ views on data sharing, and then makes the final decision by associating the aggregated outlook with a pre- quantified threshold. The more the user trusts a consumer, the more the user values the consumers' opinion. If a user agonizes a privacy loss because of the data sharing performance of another user, then the user's trust in another user diminishes. On the otherhand, since that the user needs to balance between data sharing and privacy preserving, we apply a bandit tactic to tune the threshold in the proposed trust-based mechanism, so that the user can get a high long-turn payoff which is well- defined as the difference between the advantage from posting data and the privacy loss caused by other users. We have led imitations on synthetic data and real-world data to verify the probability of the planned methods. And by harnessing the proposed UCB policy to reveal the threshold, the user can get elevated payoffs than setting the threshold to a fixed or random value.

VI REFERENCES

[1] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for onlinesocial networks: challenges and opportunities," IEEE Network, vol. 24,no. 4, pp. 13–18, July 2010.

[2] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security inbig data: Privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176,2014.

[3] L. Xu, C. Jiang, Y. Chen, J. Wang, and Y. Ren, "A framework forcategorizing and applying privacy-preservation techniques in big data mining," Computer, vol. 49, no. 2, pp. 54–62, Feb 2016.

[4] M. Qiu, K. Gai, and Z. Xiong, "Privacy-preserving wirelesscommunications using bipartite matching in social big data,"Future Generation Computer Systems, 2017.[Online].Available:http://www.sciencedirect.com/science/article/pii/S01
67739X17301449

[5] C. Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. Hutto,S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A.S. Bruckman,
[6] M. De Choudhury, and E. Gilbert, "What (or who) is public?:Privacysettings and social media content sharing," in Proceedings of the 2017ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp. 567–580.

[7] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy managementin social networks," in Proceedings of the 18th ACM InternationalConference on World Wide Web, April 2009, pp. 521–530.

[8] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacyconflicts for collaborative data sharing in online social networks," inProceedings of the 27th ACM Annual Computer Security ApplicationsConference, December 2011, pp. 103–112.

[9] J. M. Such and N. Criado, "Resolving multi-party privacy conflicts insocial media," IEEE Transactions on Knowledge and Data Engineering,vol. 28, no. 7, pp. 1851–1863, July 2016.

[10] P. Auer, N. Cesa-Bianchi, and P. Fischer, "Finite-time analysis of themultiarmed bandit problem," Machine learning, vol. 47, no. 2-3, pp.235–256, 2002.

[11] H. Hu, G.-J. Ahn, Z. Zhao, and D. Yang, "Game theoretic analysis ofmultiparty access control in online social networks," in Proceedings ofthe 19th ACM Symposium on Access Control Models and Technologies,New York, NY, June 2014, pp. 93– 102.

[12] H. Hu, G. J. Ahn, and J. Jorgensen, "Multiparty access control foronline social networks: Model and mechanisms," IEEE Transactions onKnowledge and Data Engineering, vol. 25, no. 7, pp. 1614–1627, July2013.

[13] N. Vishwamitra, Y. Li, K. Wang, H. Hu, K. Caine, and G.-J. Ahn,"Towards pii-based multiparty access control for photo sharing in onlinesocial networks," in Proceedings of the 22Nd ACM on Symposium onAccess Control Models and Technologies, June 2017, pp. 155–166.

[14] P. Mehregan and P. W. Fong, "Policy negotiation for co- owned resourcesin relationship-based access control," in Proceedings of the 21st ACMon Symposium on Access Control Models and Technologies, June 2016,pp. 125–136.

[15] J. Golbeck, "Trust on the world wide web: A survey," Foundations andTrends in Web Science, vol. 1, no. 2, pp. 131– 197, 2008.

[16] S. Zakhary, M. Radenkovic, and A. Benslimane, "Efficient locationprivacy-aware forwarding in opportunistic mobile networks," IEEETransactions on Vehicular Technology, vol. 63, no. 2, pp. 893–906, February 2014.

Authors Profile

Vennela.A is working as an Assistant Professor of CSE Department in **Qis Institute of Technology, Ongole, Prakasam (Dt)**

Nagaraju.J pursuing B Tech in computer science engineering from **Qis Institute of Technology, Ongole, Prakasam (Dt)**

Syamsundar.T pursuing B Tech in computer science engineering from **Qis Institute of Technology, Ongole, Prakasam (Dt)**

Sriharshavardhan.B pursuing B Tech in computer science engineering from **Qis Institute of Technology, Ongole, Prakasam (Dt)**

Srikanth.N pursuing B Tech in computer science engineering from **Qis Institute of Technology, Ongole, Prakasam (Dt)**

Prudhvi.M pursuing B Tech in computer science engineering from **Qis Institute of Technology, Ongole, Prakasam (Dt)**