International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183827

Conflict Detection Techniques for Preserving Privacy in Social Media

Fulpagare Priya K.*, Prof. Dr. Nitin N. Patil
Department of Computer Engineering, R. C. Patel Institute of Technology, Shirpur, Maharashtra, India

ABSTRACT

Social Network is an emerging e-service for Content Sharing Sites (CSS). It is an emerging service which provides reliable communication. Some users over CSS affect user's privacy on their personal contents, where some users keep on sending annoying comments and messages by taking advantage of the user's inherent trust in their relationship network. Integration of multiple user's privacy preferences is very difficult task, because privacy preferences may create conflict. The techniques to resolve conflicts are essentially required. Moreover, these methods need to consider how users would actually reach an agreement about a solution to the conflict in order to offer solutions acceptable by all of the concerned users. The first mechanism to resolve conflicts for multi-party privacy management in social media that is able to adapt to different situations by displaying the enterprises that users make to reach a result to the conflicts. Billions of items that are uploaded to social media are co-owned by multiple users. Only the user that uploads the item is allowed to set its privacy settings (i.e. who can access the item). This is a critical problem as users' privacy preferences for co-owned items can conflict. Multi-party privacy management is therefore of crucial importance for users to appropriately reserve their privacy in social media.

Keywords : Social Media; Content Sharing Sites, Privacy, Conflicts, Meta Data, CSS, A3P.

I. INTRODUCTION

Social media (SM) has become one of the most important parts of our daily life as it allows us to communicate with different groups of people. Social Networking (SN) is an improving technology with millions of people participating in exchanging their content as text, image, audio, video etc. Some of the social networks like Facebook, Twitter and LinkedIn are available across the internet over the past several years. These networks provide different features to the customers like chatting, posting comments, image sharing, video chatting etc. Through this SM, users may engage with each other for various purposes like business, leisure and knowledge sharing. People use social networks to get in touch with further people and create and contribute content that includes personal information, images, and videos etc. [1].

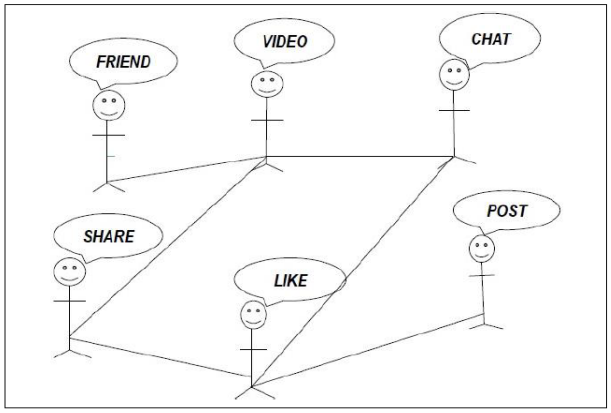

Figure 1: Activities in Social Networking Sites

There is recent suggestion that users very often assign collaboratively to achieve an agreement on privacy settings for co-owned information in social media. In particular, users are known to be generally open to accommodate other users' preferences. Also they are willing to make some concessions to reach an agreement depending on the specific situation. However, current social media privacy controls solve this kind of situations by only applying the sharing preferences of the party that uploads the item. Thus the users are forced to negotiate manually using other means such as e-mail, SMSs, phone calls etc. For example "A" and "B" may exchange some e-mails to discuss whether or not they actually share their photo with "C". The problem with this is that assigning manually all the conflicts that appear in the everyday life may be time-consuming because of the high number of possible shared items and the high number of possible targets to be considered by users; e.g., a single average user in Facebook has more than 150 friends and uploads more than 25 photos. When metadata information is unavailable it is difficult to generate accurate privacy policy. This is the disadvantage of existing system. Privacy violation as well as inaccurate classification will be the consequence of manual creation of metadata log information [2], [3].

The main purpose of Adaptive Privacy Policy Prediction [A3P] is to help users make privacy setting for their images. The possible indicators of user's privacy preferences are social-context, image-content and metadata. This A3P system examines the role of the user's privacy preferences. Conflict detection process involves two major factors.

1. If a user uploaded images consecutively or randomly then there is need to check the privacy policies of all the images.
   e.g. - If there are 10 images to be uploaded on a website then it is necessary to check what kind of privacy policies of all the images are to be applied.
2. Also if new user is added for these images then not only need to check privacy policy but also to check if there are any conflicts found or not. Check out all the conflicts so as to protect the content.

The existing systems have totally different goals to this approach. The existing approach only focuses on sharing of the content rather than protecting the content.

II. LITERATURE SURVEY

In this section, we conduct literature survey of work done till now in this domain. Our literature survey is an independent summary of published research literature relevant to the topic of our consideration.

Sundareswaran *et al.* have proposed an Adaptive Privacy Policy Prediction (A3P) system to help users combine privacy sites for their images. The proposed A3P system is comprised of two main building blocks: A3P- Social and A3P-Core. The A3P-core focuses on examining each individual user's own images and metadata, while the A3P-Social offers a community perspective of privacy setting recommendations for a user's potential privacy improvement. They designed the interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice. The renovated version of A3P is presented, which includes an prolonged policy prediction algorithm in A3P-core, and a new A3P-social module that improves the opinion of social context to refine and extend the prediction power of the system [1].

Yu *et al* introduced an automated recommendation system for a user's images to suggest suitable photo-sharing groups. Usage of social media's increased

noticeably in today world facilitate the user to distribute their personal information like images with the other users. This enhanced technology leads to privacy disobedience where the users are allocated large volumes of images across additional number of people. To provide security for the information, mechanical explanation of images are introduced which aims to create the meta data information about the images by using the novel approach called Semantic interpret Markovian Semantic Indexing(SMSI) for repossess the images [2].

Danezis *et al.* have suggested that social networking sites have upraised the risks for privacy protection because of the centralism of vast amounts of user data, the understanding of personal information collected, and the accessibility of up-to-date data which is constantly tagged and formatted. This makes social networking sites an attractive target for a variety of organizations seeking to aggregate large amounts of user data, some for real purposes and some for malicious ones [3].

Adu-Oppong *et al.* have developed privacy setting based on a concept of "Social Circles". Social networks have grown in size, and as the term "friend" has become large-scale, it has become increasingly difficult for users to control which friends get to see what personal information. In spite of the privacy controls available on such social-networking services, many users inattention to control their privacy because it is difficult to set privacy policies [4].

Yeung *et al.* claimed that mostly photo sharing sites only allow users to specify whether a photo is public, private or visible to their family members or friends. Users can only apply this setting to an individual photo or a particular set of photos. It is not possible to share photos with only, for example, one's colleagues or people who participated in a particular event. Users may also have to compile their lists of friends again if they move to another photo sharing site. Given that tags are extensively used on photos on these Web sites, and that they provide rich information of what the photos are about, it is possible to provide better access control mechanism based on the tags assigned to the photos [5].

Mazzia *et al.* proposed a privacy expert to help users allow privileges to their friends. The expert requests users to first allocate privacy labels to particular (selected) friends, and then uses this as input to form a classifier which classifies friends based on their profiles and repeatedly assign privacy labels to the unlabeled friends [6].

Strater *et al.* have evolved Online Social Network (OSN). OSN evolved into a social phenomenon on websites such as MySpace.com and Facebook.com, with approximately 110 million and sixty million active users on the sites respectively. The benefits of these sites include connecting with and support personal connections, both with friends already known offline and with people known only nearly. As part of their contribution in these online societies, Internet users are illuminating a large amount of personal information to manage their identity and build social resources. Users may relate their interests, contact information, photos, daily activities, suggestions and interfaces with other users and groups, and more [7].

Sundaram *et al.* have given various examples of some social networking sites. Social network data characteristics exclude simple signs of the social context. First, social media data typically involves multiple social relations. In Flickr for example, there are several relations including friendship or commenting relation, tagging or "like" relation, photo-to-location relationship, photo-to-time relationship. Second, the activity forms in social media often reproduce not just a single user's tedious performance and interests, but the open assembly. In Facebook and Twitter, for example, people occur due

to users' topical interests and association on projects. In Flickr, media and ideas are shared within societies of friends. Appreciative social media pleased requires awareness about people which convey related environment [8].

Barsky *et al.* have proposed numerous approaches to select "high quality" photographs assess photographs based on image qualities such as degradation caused by noise distortion, and artifacts. With the current common use of digital cameras, the process of selecting and preserving personal photographs is becoming heavy task. To address the growing number of photographs and browsing time, it is desirable to discard unattractive photographs while retaining visually pleasing ones. Due to the time-consuming nature of this process, it would be useful to have computation-based solutions to assist in photograph preservation. However, since the assessment of photographs is independent and involves personal taste, any solution based on calculation will face experiments and complications [9].

Squicciarini *et al.* have described the work based on an incentive mechanism where users are rewarded with a quantity of numeraire each time they share information or acknowledge the presence of other users (called co-owners)who are affected by the same item. When there are conflicts among co-owners' policies, users can spend their numeraire bidding for the policy that is best for them [10].

Fong *et al.* have been proposed numerous access control scheme to support fine-grained authorization specifications for OSNs. Unluckily, these schemes can only allow a single checker, the resource owner, to specify access control policies. Definitely, a flexible access control mechanism in a multi-user environment like OSNs should allow multiple checkers, who are associated with the shared data, to specify access control policies [11].

Hongxin *et al.* have been introduced an approach to permit the protection of shared data associated with multiple users in OSNs. Based on this frame an access control model to capture the core of multiparty authorization wants, along with a multiparty policy specification scheme and a policy implementation mechanism [12].

Emiliano *et al.* have been provided a systematic solution to facilitate collaborative management of shared data in OSNs. This initiate by observing how the lack of multiparty access control (MPAC) for data sharing in OSNs can weaken protection of the user data. An architecture (called Hummingbird) that offers a Twitter-like service with increased privacy guarantees for tweeters and followers equally. Hummingbird architecture mirrors Twitter's, which involve one central server and a random number of registered users, that can publish and recover short text-based messages. Publication and recovery is based on the set of hash tags that are attached to the message or specified in the search criteria [13].

Li weng *et al.* have been given a privacy protection framework is proposed for large-scale content-based information retrieval. It offers two layers of protection. First, robust hash values are used as queries to prevent enlightening original content or features. Second, the client can choose to ignore certain bits in a hash value to further increase the doubt for the server. The results show that the privacy development slightly improves the recovery performance [14].

III. METHODS AND MATERIAL

In this section, we describe the possible modifications in existing methods. Firstly some drawbacks or limitations are taken into considerations followed by understanding the advantages of enhanced system. The most widespread issues and threats objectives are

explained in different CSS appropriately. In CSS, privacy is frequently a key apprehension by the users. As millions of people are willing to interrelate with others, it is also a new worry ground for image misuses which can lead to dispersing the images and contents. The most widespread issues and threats are targeting different CSS today. It requires the precise privacy policy scheme. This suggests a privacy policy forecast and access boundaries along with overcrowding scheme for social sites using data mining techniques. It helps to detect and defend distrustful activates, which violates user's privacy in CSS by making an allowance for the following parameters [4, 5].

1. Text annotation, which emerge in the uploaded contents;
2. Image and policy descriptions;
3. Detection of superfluous commends and to perform this, the system utilizes APP (Access Policy Prediction) and
4. Access control mechanism (mediator) [6, 7].

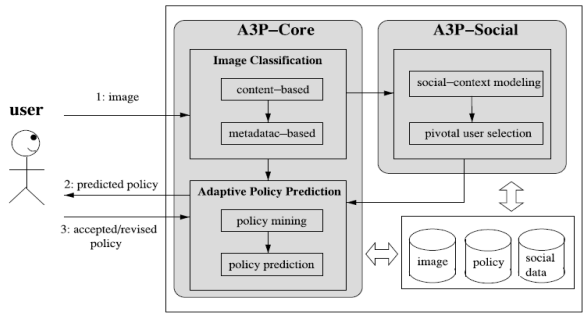

Figure 2 : A3P System Architecture.

With the reference of figure 2, in Adaptive Privacy Policy Prediction (A3P) system the personalized policies can be automatically generated by the system. It makes use of the uploaded images by users and a hierarchical image classification is done. Image content and metadata is handled by the A3P system. It consists of two components: A3P Core and A3P Social. The image will be first sent to the A3P-core, when the user uploads the image. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. When metadata information is unavailable it is difficult to generate accurate privacy policy. This is the disadvantage of this system. Privacy violation and inaccurate classification will be the later effect of manual creation of metadata log information [8, 9].

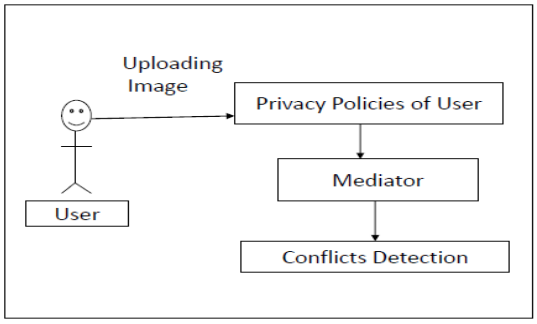

Figure 3: Modified Architecture

As per figure 3, the use of a mediator which detects conflicts, suggests a possible solution to them. Probably in most social media infrastructures, such as Facebook, Twitter, Google+ and the like, this mediator could be integrated as the back-end of SM privacy controls' interface; or it could be implemented as a social media application such as a Facebook app that works as an interface to the privacy controls of the underlying social media infrastructure. The figure 3 depicts an overview of the proposed mechanism. The mediator follows the process as [10, 11]:

1) The mediator inspects the individual privacy policies of all users for the item and flags all the conflicts found. Basically, it looks at whether individual privacy policies suggest contradictory access control decisions for the same target user. If conflicts are found the item is not shared preventively.

2) The mediator proposes a solution for each conflict found. The mediator estimates how willing each assigning user may be to grant by considering: her

individual privacy preferences, how sensitive the particular item is for her, and the relative importance of the conflicting target users for her [12, 13, 14].

IV. RESULTS AND DISCUSSION

For the performance evaluation of privacy preservation in social media, the system is executed on configuration having Windows 7 or later version with 4GB RAM. This method is implemented in JAVA. For this system JSP works on a front end and MySQL on the back end. JSP is used to store all code which we generate in implementation phase. The system implemented as a Java file embedded in an open source content management site, deployed using an Apache server.

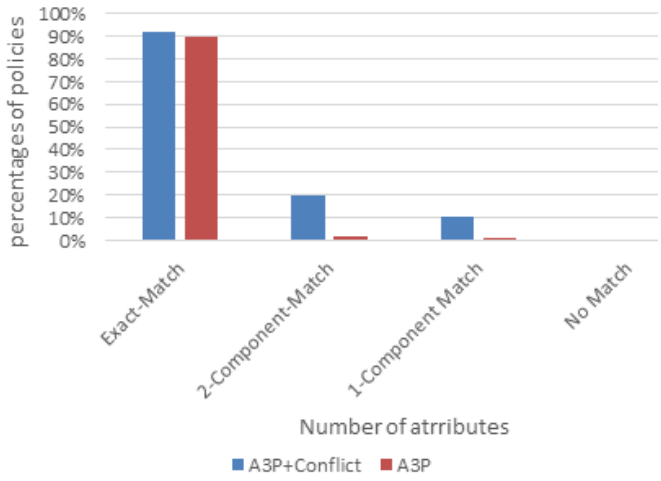

Figure 4 : Comparative Graph for component Matching

The analysis of work is supported with the following graph as shown in figure 4. From above discussion it is clear that the existing system is although effective system for circulation or for use but lack of some information creates wrong policies. The A3P-social and A3P-core are the main aspects of the system. When user uploads the image, the image will be first sent to A3P-core. The work of A3P-core classifies the image and check whether there is a need to invoke the A3P-social. In image classification the image is classified on content based data and metadata based data.

Privacy policies are automatically generated by the system. If this metadata based information is not available, it is difficult to generate accurate privacy policy. This is the drawback of the system to be overcome. This inaccurate privacy creation classification will be the consequence of manual creation of metadata log information.

- **Modified Approach :**

The A3P-core involves two type classification that are content based classification denoted as Content-mining and policy mining classification denoted as tag-mining. The collection of real user policies over made here. “Exact Match” means a predicted policy is exactly the same as the real policy of the same image; “x-component Match” means a predicted policy and its corresponding real policy have x components fully matched; “No match” simply means that the predicted policy is wrong for all components. Components are subject, action and condition. In social networking sites the various actions are performed. That are searching, tagging, comment etc. Suppose searching option will be taken into consideration. The searching mainly is based on two parameters that are search on the basis of keyword and search on the basis of content (description).

a. In keyword based search approach, title or id are the two attributes to be used. If the image id or title is matched with our content then the privacy is preserved otherwise no match indicates the policy is to be unpreserved causing generation of conflicts.
b. In content based search approach, the description of the image is used. Both these search approaches are totally different from each other. For measuring the performance of result, the following graphs are implemented.

Table 1: Contents of Component Matching

Sr. No.	Attributes	A3P+Conflict	A3P
1	Exact-Match	92%	90%
2	2-Component-Match	20%	2%
3	1-Component Match	10%	1%
4	No Match	0%	0%

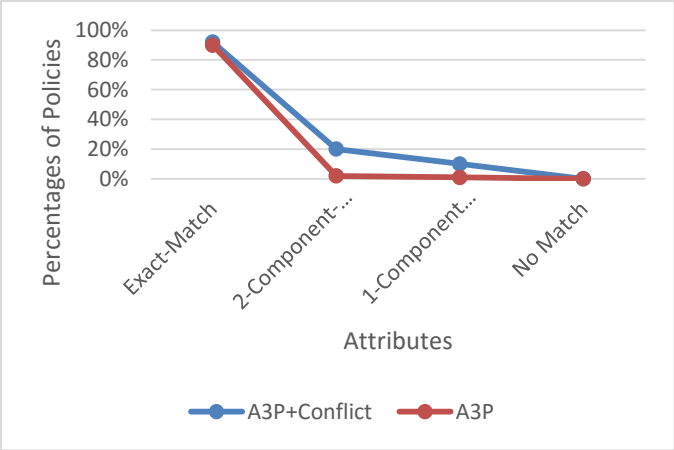

Figure 5: Comparison of Existing System and Modified Approach

The figure 4 and 5 represents the comparison of existing approach and modified approach. In comparison of existing system, the conflict detection and resolution is a technique to avoid the contraction. When inaccurate policies are generated i.e. overlapping of privacy is there, the conflict detection is required. This conflict detection technique will improve the efficiency of the existing system.

V. CONCLUSIONS AND FUTURE WORK

The goal of this paper is to describe the privacy policy resolving techniques for user uploaded data images in various content sharing sites. Based on the user social behavior and the user uploaded image, the privacy policy can applied. First mechanism for detecting privacy conflicts in social media that is based on current empirical suggestions about privacy consultations and disclosure driving factors in social media is discussed accordingly. This mechanism is also able to adapt the conflict resolution strategy based on the particular situation. In a nutshell, the mediator firstly inspects the individual privacy policies of all users involved looking for possible conflicts. If conflicts are found, the mediator recommends a solution for each conflict according to a set of franchise rules that model how users would actually assign in this domain.

The work done described in this paper is a stepping stone towards more automated resolution of conflicts in multi-party privacy management for social media. In future, we continue to work on what makes users agree or not while solving conflicts in this domain.

VI. REFERENCES

[1] Squicciarini, S. Sundareswaran, D. Lin, and J. Weed. "A3P: adaptive policy prediction for shared images over popular content sharing sites." In *Proceedings of the 22nd ACM conference on Hypertext and hypermedia*, pages 261–270. ACM, 2011.

[2] 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, 2009, pp.1464–1467.

[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] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data," in *Proc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp.*, 2009, pp. 9–14.

[6] A. Mazzia, K. LeFevre, and A. E., "The PViz comprehension tool for social network privacy settings," in *Proc. Symp. Usable Privacy Security*, 2012.

[7] K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," in *Proc. Brit. Comput. Soc. Conf. Human-Comput. Interact.*, 2008, pp.111–119.

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

[9] C.-H. Yeh, Y.-C. Ho, B. A. Barsky, and M. Ouhyoung, "Personalized photograph ranking and selection system," in *Proc.Int. Conf. Multimedia*, 2010, pp. 211–220.

[10] A. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in WWW. ACM, 2009, pp. 521–530.

[11] P. Fong, M. Anwar, and Z. Zhao, "A privacy preservation model for facebook-style social network systems," in Proceedings of the 14th European conference on Research in computer security, pages 303–320. Springer-Verlag, 2009.

[12] Hongxin Hu, Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Jan Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms," IEEE transactions on knowledge and data engineering, vol. 25, no. 7, july 2013.

[13] Emiliano De Cristofaro PARC, Claudio Soriente ETH Zurich , Gene Tsudik Andrew Williams UC Irvine UC Irvine 2012 IEEE Symposium on Security and Privacy "Hummingbird: Privacy at the time of Twitter".

[14] Li Weng, Member, IEEE, Laurent Amsaleg, April Morton, and Stéphane Marchand-Maillet, "A Privacy-Preserving Framework for Large-Scale Content-Based Information Retrieval"- IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015.