IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

A Survey on Collaborative Privacy Management of Online Photo Sharing

K C Shashwathi[1], M Natesh[2]

PG Scholar, Department of CSE, Vidya Vardhaka College of Engineering, Mysuru, India[1]

Associate Professor, Department of CSE, Vidya Vardhaka College of Engineering, Mysuru, India[2]

Abstract: Online Social Networks (OSNs) are popular because of its attractive photo sharing feature among the users. The protection of a person's private information in online social networking sites like Facebook poses a new challenge. OSNs allow users to restrict access to shared data, but they do not provide any mechanism to enforce privacy over images with multiple users. So, establishing effective method to control personal data and maintain privacy is of great importance within these OSNs. To prevent possible leakage of photo privacy, we enable each individual in a photo to be aware of photo posting activity and participate in decision making of photo posting. This paper reports, a tool called Collaborative Privacy Management (CoPE) which involves content stake-holders in managing privacy policies and ensuring protection of shared photos. Thus OSNs will protect the privacy of true user and provide secure way of sharing a photo. Hence OSNs will be safe and secure.

Keywords: Online Social Network, Photo Privacy, Photo Sharing, Collaborative Privacy Management.

I. INTRODUCTION

Online Social Networking sites have become important part of our daily life. Also the emergence of web 2.0 has brought with it the concept of Online Social Networks (OSNs). According to [1], in 2008, more than 40% of Internet users were members of at least one OSN. Recent figures show that, Facebook alone had 845 million users [2] at the end of 2011. The success of Social Networking sites like Facebook depends on the size of its users and the time they spend on Online Networking. These sites allow their members to post data containing personal information, customize them as they wish to express themselves, socialize and interact with others. Users, however, are often unaware of the numbers or nature of the audience that could potentially access their personal data. The availability of personal data potentially exposes users to a number of security and privacy risks [3, 4]. The first decade of 21st century has seen an extreme rise in the size of the Internet users and the growth of Web Services which helps in the information sharing and collaboration.

A user profile in any OSN usually includes information such as profile name, birthday, sex, residence, interests, education and travel information. But according to a research, simple disclosure of birth date and place of birth of a profile in Facebook can be used to predict Social Security Number (SSN) of a citizen in the US. And also users upload photos and tag other people even though they are not willing to be a part of the uploaded content. Many privacy concerns may arise from this practice. Such collaborative activities give to a new set of privacy challenge because here a person's private information can be easily revealed in content created by others. In other words, private information will not only reside in a single user's own domain but also co-owned and co-managed by other stake-holders. So far, there is no restriction with sharing of co-photos, on the converse, Social Network service providers such as Facebook are encouraging users to post co-photo and tag their friends in order to get more people involved. We need to enforce maximum level of privacy and security of the content being uploaded on OSNs. So while using the OSNs its user should feel a desired level of security and confidence. The user should use it without worrying or content being shared in unauthorized and insecure way. For the user using online social sites, the desired level of privacy and security is an important thing.

This paper proposes a system based on novel consensus, approach to achieve privacy and efficiency at the same time. And also here exposure and privacy policies are used which defines the overall audience who can be given access to uploaded image. We pursue a systematic solution to facilitate collaborative management of shared data in OSNs which gives control over their personal and private information. We seek to add to the growing privacy literature by providing a conceptual understanding of Collaborative Privacy Management (CoPE) system, to support users.

The rest of this paper is structured as follows. In the next section, we briefly review the background and related work. And later, we have discussed our collaborative privacy management approach. Finally in the last section, we conclude our research and discuss the potential future research.

II. RELATED WORK

Privacy is a big a concern in Online Social Networks (OSNs). This section summarizes some of the relevant research, in particular from the privacy protection perspective in OSNs and privacy related information sharing at the group level.

DOI 10.17148/IJARCCE.2016.5465

A number of studies have highlighted the privacy issues in OSNs. In a study [5], on Norwegian users on Facebook has shown that users knowledge on how social media functions in regard to personal information is mostly inadequate. And in another study [6], it was found that every one of the participants had at least one sharing violation on the shared content in OSNs.

Photo tagging is a popular feature of many OSNs, in [7], we examined the privacy concerns and mechanisms for tagged images. Even if through the photo tags [11], if the individual is not identified, someone's identity can be inferred through the publicly available data and combination face recognition software.

Several studies reveal the privacy attitudes of the users of OSNs [8, 9] and the possible risks that the users face when they fail to adequately protect their information on social sites. Thus, the current privacy management systems ensure information be shared according to their privacy interests.

Many systems proposed privacy preserving methods on OSNs. Rule based access control [10] presents a system that consists of policies in the form of constraints on the type, depth and trust level of the relationship that are existing for web-based social networks (WBSNs). A rule-based access control model is proposed for WBSNs, which allows the requirement of access rules for online resources where the relationship between authorized users in the network is denoted in terms of the relationship type, depth, and trust level. Pviz comprehension tool [11] explains how users model groups and privacy policies applied to their networks. It is an interface that allows the user to understand its profile based on natural grouping of friends. Privacy settings based on the concept of social circles [12] which protects personal information through a web based solution was developed. Here friend's lists are automatically generated by social circles finder. An access control system [13] based on a descriptive tags and linked data of social networks in the semantic web. It allows users to create policies for their photos and users can specify access control rules. Adaptive Privacy Policy Prediction (A3P) system [14], generates policies that are personalized automatically as it is a free system. Based on the content, personal information and metadata, the user's uploaded images can be handled by A3P system. Finally, most of these approaches have concentrated on a single-user-centred solution and has failed to recognize the need for privacy actions by groups. The implication is that privacy management is not just a matter for the exercise of actions but also an aspect of collaborative actions.

Privacy concerns in collaboration have been studied in the area of Computer-Supported Collaboration Work (CSCW). The privacy issues in CSCW are very different from that Collaboration Privacy Management (CoPE) in an OSN, concerned private information can be owned by more than one user. In CSCW, only one user can control the access to private data. In OSN, it has heterogeneous relationships, while CSCW often is concerned with small groups. Thus current research on privacy management cannot fully address the needs for CoPE in OSNs. New designs are needed to help the user to manage private information effectively by self and with others.

III. DISCUSSION

Online photo sharing is chosen as the application domain to study collaborative privacy management. One of the popular feature of Online Social Networks (OSNs) is the image sharing. The privacy concerns become particularly important in OSNs because online images are often tied to individual profile either explicitly or implicitly. Our method is to design tools that allow users to collaboratively manage their shared images on OSNs. This collaborative privacy management (CoPE) approach considers two main factors: content that needs to be protected, and stake-holders who are involved in content sharing and privacy management.

Consider a scenario where two stake-holders are involved over a shared content. The person whose privacy is revealed by a picture and the person who creates and owns the picture we can refer to the former as a privacy owner and the latter as a content owner. To manage the privacy, these two stake-holders work together in controlling the access to the picture.

We designed a tool, CoPE for Facebook users to manage the access control for photos posted. The tool provides a user with the following function:

- **Collecting images in which the user was tagged:** It allows a stake-holder to control various privacy related settings that relate to their photos. A user can set the viewable attribute of any photo to "only co-owners", "friends", and "public" to limit the potential viewers.
- **Notifying the user about tagging event:** Notifying users when they have been tagged by friends who also are using CoPE.
- **Requesting co-ownership:** Allowing users to request co-ownership on images in which they were tagged, notifying users about request on co-ownership, allowing users to grant co-ownership to others.
- **Browsing history:** CoPE allows user to keep track of who has viewed their photos.

The CoPE tool provides a proof of concept implantation of collaborative privacy management. This improves private data management and protection within OSNs. An initial application that supports new collaborative privacy control mechanisms are demonstrated here. Our approach can be generalized and used to manage privacy in other types of contents within the context of Web 2.0.

Some of the limitations of this research are that the simple mechanism to determine the stake-holders may rise an issue of trust, stake-holders are not necessarily related to each other, may create opportunities for abnormal activities, the way to control viewers in our design may not be as comprehensive as what users need, and our

DOI 10.17148/IJARCCE.2016.5465

approach may not return the most appropriate collective policy in certain scenarios.

IV. CONCLUSION

Photo sharing is the process of publishing or transfer of a user's digital photos on online. We have observed that the problems related to collaborative privacy management present long term challenges. This research is one of first attempt to model Collaborative Privacy management (CoPE).

The design and implementation of CoPE system can be enhanced in several ways. Like applying this approach in different type of online contents. In addition, increasingly sophisticated approaches for stake-holder detection may also be developed and deployed. It is also important to investigate the ways in which the present approach protects itself from malicious user or those who enforce only their own preferences. Additionally, other aspects of CoPE should be assessed in the future research.

REFERENCES

[1]. S. Gurses, R. Rizk, and O. Gunther. Privacy design in online social networks: Learning from privacy breaches and community feedback. In ICIS 2008 Proceedings, New York, USA, 2008. ACM.

[2]. http://techcrunch.com/2012/02/01/facebooks-s-1-845-million-users.

[3]. Gross, R., and Acquisti, A. "Information revelation and privacy in online social networks," Workshop on Privacy in the Electronic Society, 2005.

[4]. Rosenblum, D. (2007). What Anyone Can Know: The Privacy Risks of Social Networking Sites. IEEE Security and Privacy 5(3), pp 40-49.

[5]. P. B. Brandtzaeg and M. L□uders. Privacy 2.0: Personal and consumer protection in new media reality. Tech. Rep. SINTEF A12979, Nov'09.

[6]. M. Majeski, M. Johnson, and S. M. Bellovin. The failure of online social network privacy settings. Technical Report CUCS-010-11, Feb. 2011.

[7]. A Paper on "Moving Beyond Untagging: Photo Privacy in Tagged World" AUTHORS: Andrew Besmer& Heather Richter Lipford. Department of Software and Information Systems.

[8]. Acquisti, A. & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Proc. of Privacy Enhancing Technologies Symposium, pp. 36-58.

[9]. Hoadley, C., Xu, H., Lee, J. & Rosson, M. B. (2010). Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry. Electronic Commerce Research and Applications (forthcoming).

[10]. B. Carminati, E. Ferrari, and A. Perego, "Rule-based access control for social networks", Springer Berlin Heidelberg, Vol.278, pp.1734- 1744, 2006.

[11]. Z. Stone, T. Zickler, and T. Darrell, "Autotagging facebook: Social network context improves photo annotation", IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp. 1-8, 2008.

[12]. Alessandra Mazzia Kristen LeFevre and Eytan Adar, "The PViz Comprehension Tool for Social Network Privacy Settings", Tech. rep., University of Michigan, 2011.

[13]. C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data", pp. 9–14, 2009.

[14]. Anna Cinzia Squicciarini, "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites", IEEE Transactions on Knowledge And Data Engineering, Vol. 27, no. 1, January 2015.

[15]. Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova , "I Know What You Did Last Summer!:Privacy-Aware Image Classification and Search ", Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval, 2012.

DOI 10.17148/IJARCCE.2016.5465