IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 48-52
www.iosrjournals.org

User Shared Images For Social Media With Preserving Privacy Policy Models

Miss M.Malathi[1], Mrs M.Valarmathi[2]
M.Sc,M.Phil Full Time Scholar.,Department of Computer Science,Vivekanandha College for Women.
E-Mail id:malathi94bca@gmail.com.
MCA, M.Phil., Assistant Professor Department of Computer Science, Vivekanandha College for Women.
E-Mail id:valardhaanu2006@gmail.com.

Abstract: *Online social networks (OSNs) such as Facebook, Google+ and Twitter are inherently designed to alter individuals to share personal and public data and build social connections with friends, coworkers, colleagues, family and even with strangers. In recent years, it has seen unprecedented growth in the application of OSNs. An interesting phenomenon of user shared images is observed from the intensive measurements, and this is formulated with a proposed method for a system to discover and recommend user connections in follower/followed relationships using user shared images directly.In this paper keep the information of social graphs (SGs) available to their related business services. Some users also hide or border the information of their connections from the public in social media platforms due to privacy concerns. Accessing these SGs is getting more difficult and costly in today's online social networks and novel applications using SGs become almost impossible to be offered independently by third-party practitioners and individuals. However, billions of user shared images are generated by people in several social networks daily and this particular form of user data is indeed very accessible to others as a result of the character of on-line image sharing. This paper also proposes an approach to enable the protection of shared data associated with multiple users in OSNs. An access control model is formulated to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, it present a logical representation of the access control model that allows us to leverage the features of existing logic solvers to perform various analysis tasks on the model.*

Keywords: *Online Social Networks, Recommendation, On-line image sharing, social graphs, connection.*

I. Introduction

The papers leverages traditional group-based policy management as our baseline and progressively improve upon this privacy management model. With each new enhancement, we measure their human effects including cluster/user defined relationship group alignment, user privacy sentiment, efficiencies and user perceptions. The thesis introduces a user-assisted friend grouping mechanism that enhances traditional group-based policy management approaches.

Assisted Friend Grouping leverages established clustering techniques to aid users in grouping their friends more effectively and efficiently. It introduces a new privacy management model that is an improvement over traditional group-based policy management approaches. The new paradigm leverages a user's memory and opinion of their friends to set policies for other similar friends, which we refer to as Same-As Policy Management. Users associate the policy with an example friend and in doing so have this friend in the forefront of their mind. This allows users to be more selective and careful in assigning permissions. Users are thinking of people, not groups. Using a visual policy editor that takes advantage of friend recognition and minimal task interruptions, Same-As Policy Management demonstrated improved performance and user perceptions over traditional group-based policy management approaches.

It further enhances Same-As Policy Management by introducing Example Friend Selection—two techniques for aiding users in selecting their example friends that are used in developing policy templates. Both techniques reduced policy authoring times and were positively perceived by users. In addition, the thesis proposes an approach to enable the protection of shared data associated with multiple users in OSNs.

II. Literature Survey

T. Ristenpart stated that the existence of online social networks that include person specific information creates interesting opportunities for various applications ranging from marketing to community organization. On the other hand, security and privacy concerns need to be addressed for creating such applications. Improving social network access control systems appears as the first step toward addressing the existing security and privacy

concerns related to online social networks. To address some of the current limitations, they have created an experimental social network using synthetic data which they then used to test the efficacy of the semantic reasoning based approaches they have previously suggested.

Y. Zhang stated that users and resources in online social networks (OSNs) are interconnected via various types of relationships. In particular, user-to-user relationships form the basis of the OSN structure, and play a significant role in specifying and enforcing access control. Individual users and the OSN provider should be allowed to specify which access can be granted in terms of existing relationships.

They proposed a novel user-to-user relationship-based access control (UURAC) model for OSN systems that utilizes regular expression notation for such policy specification. They developed a path checking algorithm to determine whether the required relationship path between users for a given access request exists, and provide proofs of correctness and complexity analysis for this algorithm.

J. Somorovsky stated that Privacy is an enormous problem in online social networking sites. While sites such as Facebook allow users fine-grained control over who can see their profiles, it is difficult for average users to specify this kind of detailed policy.

In this paper, they proposed a template for the design of a social networking privacy wizard. The intuition for the design comes from the observation that real users conceive their privacy preferences (which friends should be able to see which information) based on an implicit set of rules. Thus, with a limited amount of user input, it is usually possible to build a machine learning model that concisely describes a particular user's preferences, and then use this model to configure the user's privacy settings automatically.

III. Collaborative Method

Several recommendation systems use a hybrid approach by combining collaborative and content-based methods, which helps to avoid certain limitations of content-based and collaborative systems. Different ways to combine collaborative and content-based methods into a hybrid recommender system can be classified as follows:

- Implementing collaborative and content-based methods separately and combining their predictions,
- Incorporating some content-based characteristics into a collaborative approach,
- Incorporating some collaborative characteristics into a content-based approach, and
- Constructing a general unifying model that incorporates both content-based and collaborative characteristics.

Adding Content-Based Characteristics to Collaborative Models Several hybrid recommender systems, including Fab and the "collaboration via content" approach, described in are based on traditional collaborative techniques but also maintain the content-based profiles for each user. These content-based profiles, and not the commonly rated items, are then used to calculate the similarity between two users. Recommender systems made significant progress over the last decade when numerous content-based, collaborative, and hybrid methods were proposed and several "industrial strength" systems have been developed. However, despite all of these advances, the current generation of recommender systems surveyed in this paper still requires further improvements to make recommendation methods more effective in a broader range of applications.

Collaborative tagging is currently an extremely popular online service. Although nowadays it is basically used to support resource search and browsing, its potential is still to be exploited. One of these potential applications is the provision of web access functionalities such as content filtering and discovery. For this to become a reality, however, it would be necessary to extend the architecture of current collaborative tagging services so as to include a policy layer that supports the enforcement of user preferences.

A. Tagging And Taxonomy

Collaborative tagging describes the process by which many users add metadata in the form of keywords to shared content. Recently, collaborative tagging has grown in popularity on the web, on sites that allow users to tag bookmarks, photographs and other content. In this study analyze the structure of collaborative tagging systems as well as their dynamical aspects. Specifically, discovered regularities in user activity, tag frequencies, kinds of tags used, bursts of popularity in book marking and a remarkable stability in the relative proportions of tags within a given UR and present a dynamical model of collaborative tagging that predicts these stable patterns and relates them to imitation and shared knowledge.

The Tag desirable properties of a good tagging system, which include: (a) high coverage of multiple facets, (b) high popularity, and (c) least-effort. Faceted and generic tags can facilitate the aggregation of objects entered by different users. It makes discovery and recovery of tagged content easier. Tags used by a large number of people for a given object are less likely to be spam and more likely to be used by a new user for the same object. Least-effort has two meanings:

Propose a reputation score for each user based on the quality of the tags contributed by the user. By introducing the notion of "virtual" users, our tag suggestion algorithm incorporates not only user-generated tags but also other sources of tags. Adding semantics to the e-learning contents on the web can provide several benefits to the users:

- Provide a more accessible contents for the blind and visually impaired individuals, as the contents can be read by screen readers.
- Easier searching for technical and educational materials.
- The contents can be explained (e.g., using other students annotations or from relations between other contents).
- Help people with learning disabilities in navigating the e-learning contents (e.g., providing information about a concept in the navigated e-learning as a tooltip).

According to (Bateman, 2007) collaborative tagging systems have potential to be a good fit with e-learning systems, because of the following:

- Learning managements systems currently lack sufficient support for self organization of learning content.
- Collaborative tagging has potential to further enrich peer interactions and peer awareness centered on learning content.
- Tagging, by its nature is a reflective practice, which can give students an opportunity to summarize new ideas, while receiving peer support (through viewing other learners' tags; tag suggestions).

B. Tag Suppression

In our scenario of collaborative tagging, users tag resources on the web, for example, music, pictures, videos or bookmarks, according to their personal preferences. Users therefore contribute to describe and classify those resources, but this is inevitably at the expense of revealing their profile. To avoid being accurately profiled by tagging systems or in general by any attacker able to collect such information, users may adopt a privacy-enhancing technology based on data perturbation. The data-perturbative technology considered in this work is tag suppression, a technique that allows a user to refrain from tagging certain resources in such a manner that the profile resulting from this perturbation does not capture their interests so precisely.

Proposed system conceptually simple technique protects user privacy to a certain degree, but at the cost of the semantic loss incurred by suppressing tags. Other approaches based on data perturbation include the submission of false tags. For example, a user wishing to tag the webpage www.mentalhelp.net with "depression" could use the tag "sports" instead, to conceal their interest for this resource. In doing so, the user distorts their actual profile, although at the expense of a far greater impact on semantic functionality than suppression does resources are assigned tags that do not describe, in principle, the actual content of such resources.

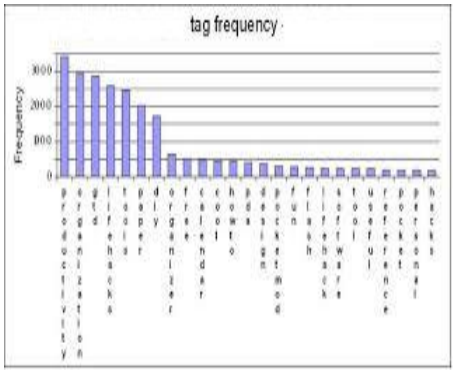

Fig 4.1 Histogram of relative frequencies of tags

C. Advantage of Collabatoive Methodology

In social network, users can allow friends to access their data, depending on their personal endorsement and privacy requirements. Although social network currently provide simple access control mechanisms allowing users to lead access to information contained in their profile, users unfortunately have no control over data. If a user posts a comment in a friend's space cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy about the photo. The existing system introduces two strategies.

- Policies for resource recommendation
- Policies for parental control

Policies for resource recommendation: Suppose that Carol (C) is interested in literature, but not in resources concerning science-fiction. C realizes that the relevant tag categories are c1 ("books") and c2 ("literary criticism"), and she decides that the resources she is interested in are those associated with not less than 40 percent of the tags in either c1 or c2. In contrast, C finds out that the tag category that corresponds to the resources she is not interested in is c3 ("science-fiction, fantasy"), and she decides to discard all the resources associated with not less than 20 percent of the tags in c3. Consequently, C specifies the following policies:

- pol1 = ({(c1, □ , 0.4)}, +),
- pol2 = ({(c2, □, 0.4)}, +),
- pol3 = ({(c3, □ , 0.2)},-)

Suppose now that there exists a resource R1, which satisfies content constraints (c1, □ , 0:4), (c2, □, 0:4), and (c3, □, 0:2). In such a case, there exists a conflict, since all policies pol1, pol2, and pol3 apply. According to the conflict resolution mechanism, policy pol3 prevails over policies pol1 and pol2, since the latter are positive policies. Consequently, resource R1 is marked as irrelevant to C.

Policies for parental control: Suppose that Alice (A) would like to enable a web filter for her son Bob (B) by granting him access only to contents specifically tailored for children. By checking the available tag categories, she realizes that the suitable one is c4: "entertainment for children." She then decides that resources suitable to children are those associated with not less than 60 percent of the tags from category c4.

pol4 = ({(c4, □, 0.6)}, +),

- pol5 = ({(c5,□ □ □0.1)},-) where c5 is the tag category corresponding to "entertainment for adults."

Suppose now that B requests access to a resource R2 which satisfies both content constraints (c4, □ , 0.6) and (c5, □ , 0.1). In such a case, there exists a conflict, since both policies pol4 and pol5 apply. According to the conflict resolution mechanism, policy pol5 prevails over pol4 because pol5 is a negative policy. Consequently, Bob is denied access to resource R2.

- Full prototype is not developed for the experimented system.
- Tags are prepared for single language (English) only.
- Tags are generalized in single level. i.e., one common word for one tag. For example, to reduce the sensitivity of the work 'depression' the word 'health' is used.

IV. Conclusion And Future Enhancement

Collaborative tagging is currently an really popular online service. Although nowadays it is basically used to support resource search and browsing, its potential is still to be exploited. One of these potential applications is the provision of web access functionalities such as content filtering and discovery. For this to become a reality, however, it would be necessary to extend the architecture of present collaborative tagging services so as to include a policy layer that supports the enforcement of user preference.

Collaborative tagging has been gaining popularity, it have been become more evident the need for privacy protection; not only because tags are sensitive information but also because of the risk of cross referencing. In addition to the existing system approaches, the proposed system takes care of multi language tagging.A privacy preserving collaborative tagging if applied to content with multiple languages, and then it becomes more effective to fruitful to end users. Future work includes the development of a full prototype for the experimented system and it's testing and use in further scenarios.

Acknowledgment

My heartfelt gratitude goes to my beloved guide Mrs M.Valarmathi, Assistant Professor, Department of Computer Science, Vivekanandha College for Women, Tiruchengode, India for dedication and patience in assigning me her valuable advice and efforts during the course of my studies.

References

[1]. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 199-212, 2009.

[2]. Y. Zhang, A. Juels, M.K.M. Reiter, and T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys," Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 305-316, 2012.

[3]. J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces," Proc. Third ACM Workshop Cloud Computing Security Workshop (CCSW '11), pp. 3-14, 2011.
[4]. S. Bugiel, S. Nu ¨ rnberger, T. Po ¨ppelmann, A.-R. Sadeghi, and T.Schneider, "AmazonIA: When Elasticity Snaps Back," Proc. 18th ACM Conf. Computer and Comm. Security (CCS '11), pp. 389-400, 2011.
[5]. G. Danezis and B. Livshits, "Towards Ensuring Client-Side Computational Integrity (Position Paper)," Proc. ACM Cloud Computing Security Workshop (CCSW '11), pp. 125-130, 2011.
[6]. S. Groß and A. Schill, "Towards User Centric Data Governance and Control in the Cloud," Proc. IFIP WG 11.4 Int'l Conf. Open Problems in Network Security (iNetSeC), pp. 132-144, 2011.
[7]. M. Burkhart,M. Strasser, D. Many, and X. Dimitropoulos, "SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics," Proc. USENIX Security Symp., pp. 223-240, 2010.
[8]. D.Hubbard and M. Sutton, "Top Threats to Cloud Computing V1.0," Cloud Security Alliance, http://www. cloudsecurityalliance.org/topthreats, 2010.
[9]. Amazon Elastic Compute Cloud (EC2).http://aws.amazon.com/ec2/
[10]. Microsoft Azure Services Platform.http://www.microsoft.com/azure/default.mspx