A Novel Approach of Multiple Access Control to Online Social Networks

Prof. Subhash V. Pingale, Mr. Sandip Sharad Shirgave

***Abstract*— Grand growth of online social networks (OSN's) in recent years and become a de facto portal for hundreds of millions of Internet users. Due to the tremendous increase of users on social network websites, the needs to assist users to manage their large number of contacts, data and information as well as providing privacy protection become more and more evident. Unfortunately, limited tools are available to address such needs and reduce users workload on managing their social relationships. Most of the online social networks such as Facebook ,which allows users to limited access to shared data, they are not providing any mechanism or any technique to provide privacy involvement over data which is related with multiple users.**

To tackle this issue, We are proposing an approach to facilitate online social network users to enable the protection of shared data associated with multiple users in OSNs.

***Index Terms*—Social network, privacy, multiple users.**

I. Introduction

Since its creation, the Internet has many information sharing networks, the most well-known of which is the World Wide Web. Recently, a new class of information networks called "online social networks" have exploded in popularity and now rival the traditional Web in terms of usage. Literally, privacy means the right to be independent of every external interruption or interference and become free by oneself. It can also be referred as the right to prevent one's personal information from being exposed to others. The Online Social Network (OSN) has shown tremendous growth in a very short span which is clear from the thing that day by day the number of OSN users is increasing .The user base of Facebook alone has crossed 800 million around the globe. Almost everyone is member of at least one of the Online Social Networks. The OSN user can easily find his friend by searching the OSN.

It is believed that Social networks have challenges for mankind as well as its opportunities has a special dynamic attribute to human social development. To provide more evidence for this point, online social networks have both positive and negative sides, definitely, it is cheaper to use online social networking for both personal and business use because most of the services are free, and at the same time, users can easily develop their social life [6]. However, for the negative side, sometimes users have to be extra-careful in using online social networks. This is because; there are many reporting cases of hacking of one's identity. Besides, this negative consequence, social networking sites (SNS) are online environments in which people create self-descriptive profiles and then make links with other people they know on the site.

The online social network (OSN) provides each user with a virtual space which contain profile information, a list of the user's friends, and webpage's, such as wall in Facebook, where users and friends can post content and leave messages. A user profile usually contains information with respect to the user's birthday, gender, interests, education, and work history, and contact information. OSN user also can not only add the information or post the information on their own wall or post the information to friends wall but also tag other users who appear in the content.[1]

OSNs currently provide simple access control mechanisms which allows users to access to data and information contained in their own spaces, users, unfortunately, there is no control over data residing outside their spaces [2]. For example, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict or cannot set the privacy setting who can see this photo, even though the tagged friends may have different privacy concerns and tagged friends having different privacy setting about the photo. Because of this limitation we are developing collaborative management for shared data in OSNs, known as MPAC model. [1]

II. Background

We begin by defining online social networks, providing a brief history of their growth

in popularity, and detail the mechanisms that today's online social networks provide for users to connect and share content.[5]

An online social network to be a system where (a) users are first class entities with a semi-public profile, (b) users can create explicit links to other users or content items, and (c) users can navigate the social network by browsing the links and profiles of other users.

Online social networks serve a number of purposes, but

***Prof. S. V. Pingale** is currently working as a professor in SKN Sinhgad College Of Engineering ,Korti, Solapur University, India,*

E-mail: sub.pingale83@gmail.com

***Mr. Sandip Sharad Shirgave** is currently pursuing master's degree program in computer science & engineering in SKN Sinhgad College Of Engineering, Korti, Solapur University, India, PH-09850004107.*

E-mail: sandipshirgave@gmail.com

ISSN: 2278 – 7798

three primary roles stand out as common across all sites. First, online social networks are used to maintain and strengthen existing social ties, or make new social connections. The sites allow users to "articulate and make visible their social networks", thereby "communicating with people who are already a part of their extended social network" . Second, online social networks are used by each member to upload her own content. Note that the content shared often varies from site to site, and sometimes is only the user's profile itself. Third, online social networks are used to find new, interesting content by filtering, recommending, and organizing the content uploaded by users.[5]

III. Literature Review

Author Imen Ben Dhia developed an access control model for OSNs that enables a fine-grained description of privacy policies. These policies are specified in terms of constraints on the type, direction, depth of relationships and trust levels between users, as well as on the users properties. This model relies on a reachability based approach, where a subject requesting to access an object must satisfy policies determined by the object owner.[3]

Author Imen Ben Dhia proposed solution aims to support users when they wish to restrict the visibility of their resources to a smaller subset of their contacts. In this paper, author propose a reachability based access control model that allows users to express their privacy preferences as constraints on existing links with other users. Experimental results verify the effectiveness of our approach over real social networks datasets.[3]

Author Jun Pang and Yang Zhang first identified a new type of access control policies that are meaningful but have never been addressed in the literature. Namely, users in social networks can express access control requirements not only based on their social relations, but also on their connections through public information. Then author Jun Pang and Yang Zhang defined a social network model containing users and public information. Based on this model, author proposed a hybrid logic to define access control policies.[8]

Author gave a number of policies based on public information and formulated them precisely in our proposed logic. In addition, author have used category relations among public information to extend our logic and make it more practical.[8]

Author Y. Cheng, J. Park, and R. Sandhu, developed an access control model for OSNs that provides finer-grained access control for users usage and administrative access by utilizing user-to-user, user-to resource and resource-to-resource relationship-based policies. These policies are specified in terms of relationship path patterns between the accessing user and the target together with hop count limit of the relationships.[4]

Specifically, author introduce the skipping of some relationship path expression in the policy specification in order to offer more expressive policies. The decision modules of the system determine authorizations by retrieving different policies from the accessing session, the target and the system, and then making a collective decision. To address policy conflicts, author apply conflict resolution policies over relationship precedence. In the future, author is planning to extend his model to incorporate attribute-based controls.[4]

Author also plan to extend our path checking algorithm of U2U relationships to cover the U2R and R2R relationships.[4]

Author Anna Squicciarini , Sushama Karumanchi , Dan Lin, Nicole DeSisto, proposed an approach which helps users in managing their social network contacts into relevant groups automatically, and also helps users set up their privacy policies automatically for their uploaded content. Organizing contacts into groups helps users set privacy settings for newly added content or new contacts joining their social circles.[6]

Authors Philip W. L. Fong and Mohd Anwar, Zhen Zhao, work takes a first step in deepening the understanding of this access control paradigm, by proposing an access control model that formalizes and generalizes the privacy preservation mechanism of Facebook. The model can be instantiated into a family of Facebook-style social network systems, each with a recognizably different access control mechanism, so that Facebook is but one instantiation of the model.[7]

Author Philip W. L. Fong and Mohd Anwar, Zhen Zhao also demonstrate that the model can be instantiated to express policies that are not currently supported by Facebook but possess rich and natural social significance. This work thus delineates the design space of privacy preservation mechanisms for Facebook-style social network systems, and lays out a formal framework for policy analysis in these systems.[7]

IV. Problem Statement

To enable the protection of shared data associated with multiple users in online social networks with the help of access control mechanism.

With the help of multiparty access control model we will implement the MController application .A core component of MController is the decision-making module, which processes access requests and returns responses (either permit or deny) for the requests.

There are three main modules which is given below.

1. Multiparty Access Control Model.
2. Multiparty policy evaluation process.
3. Decision Making Module.

V. Methodology

Multiparty Access Control (MPAC) Model

An OSN can be represented by a relationship network, a set of user groups, and a collection of user data. The relationship network of an OSN is a directed labeled graph, where each node denotes a user and each edge represents a relationship between two users. MPAC includes different controllers, owner, contributor, stakeholder, and

ISSN: 2278 – 7798

disseminator.[1]

Multiparty Access Control (MPAC) Controllers

Definition 1 (Owner): Let d be a data item in the space of a user u in the social network. The user u is called the owner of d.

Definition 2 (Contributor): Let d be a data item published by a user u in someone else space in the social network. The user u is called the contributor of d.

Definition 3 (Stakeholder): Let d be a data item in the space of a user in the social network. Let T be the set of tagged users associated with d. A user u is called a stakeholder of d, if u 2 T.

Definition 4 (Disseminator): Let d be a data item shared by a user u from someone else space to his/her space in the social network. The user u is called a disseminator of d.[1]

Multiparty Policy Evaluation Process

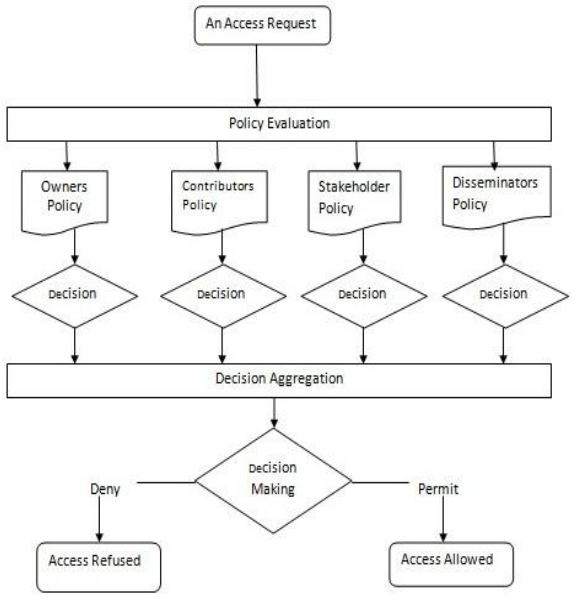

Figure 1 :- Multiparty policy evaluation process.

Above figure 1 shows the evaluation process of Multiparty Access Control (MPAC) policies. So data controllers may generate different decisions (permit and deny) for an access request, conflicts may occur. To solving unambiguous decision for each access request, it is important to adopt a perfect conflict resolution mechanism to resolve those conflicts during multiparty policy evaluation.

Privacy Conflict

Multiple controllers of the shared data item often have different privacy concerns over the data item, it leads to privacy conflicts.

VI. Solution for Privacy Conflicts

1) Majority voting for decision making

A notable feature of the voting mechanism for conflict resolution is that the decision from each controller is able to have an effect on the final decision.

2) Strategy-Based Conflict Resolution with Privacy Recommendation

The owner's decision has the highest priority. This strategy achieves the owner control mechanism that most OSNs are currently utilizing for data sharing.

A core component of MController is the decision-making module, which processes access requests and returns responses (either permit or deny) for the requests. To evaluate an access request, the policies of each controller of the targeted content are enforced first to generate a decision for the controller. Then, the decisions of all controllers are aggregated to yield a final decision as the response of the request.

VII. Conclusion

In this paper we proposed the collaborative multiple user data management mechanism in OSN. It involves multiparty policy specification and evaluation scheme. A Mcontroller is used to implement to manage multiple user privacy and security mechanisms for the user data. A privacy conflict occur due to different privacy setting, so we implement decision making module which gives the correct decision for privacy setting. This module correctly decides to whom shared information should be shown.

So, We proposed multiparty access control mechanism for multiple users to share the data in online social network in secure manner.

VIII. References

[1] Hongxin Hu, Gail-Joon Ahn, Senior 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

[2] H. Hu, G.-J. Ahn, and J. Jorgensen, "Enabling Collaborative Data Sharing in Google+",Technical Report ASU-SCIDSE-12-1, http://sefcom.asu.edu/mpac/mpac+.pdf, Apr. 2012.

[3] Imen Ben Dhia "Access Control in Social Networks : A reachability-Based Approach", EDBT/ICDT Workshops March 26-30, 2012, Berlin, Germany. Copyright 2012 ACM 978-1-4503-1143-4/12/03.

[4] Y. Cheng, J. Park, and R. Sandhu. " A user-to-user relationship-based access control model for online social networks ". In Proceedings of the 26th IFIP Annual WG 11.3 Conference on Data and Application Security and Privacy (DBSec '12), 2012.

[5] Mehmet Sahinoglua, Aysen Dener Akkayab, David Angc "Can We Assess and Monitor Privacy and Security Risk for Social Networks?", 2012. International Conference on Asia Pacific Business Innovation and Technology

ISSN: 2278 – 7798

Management.

[6] Squicciarini A, et al., "Identifying hidden social circles for advanced privacy configuration,
C" (2013), http://dx.doi.org/10.1016/j.cose.2013.07.007, www.sciencedirect.com

[7] P. Fong, M. Anwar, and Z. Zhao, "A Privacy Preservation Model for Facebook-Style Social Network Systems", Proc. 14th European Conf. Research in Computer Security, pp. 303-320, 2009.

[8] Jun Pang and Yang Zhang "A New Access Control Scheme for Facebook-style Social Networks", , arXiv:1304.2504v2 [cs.CR] 16 Dec 2013

[9] Thang N. Dinh, Yilin Shen, and My T. Thai. "The Walls Have Ears: Optimize Sharing for Visibility and Privacy in Online Social Networks" CIKM'12, October 29–November 2, 2012, Maui, HI, USA. Copyright 2012 ACM 978-1-4503-1156-4/12/10 ...$15.00.

[10] Karr-Wisniewski, Pamela; Wilson, D; and Richter-Lipford, "A New Social Order: Mechanisms for Social Network Site Boundary Regulation" (2011). AMCIS 2011 Proceedings - All Submissions. Paper 101. http://aisel.aisnet.org/amcis2011_submissions/101

[11] Victoria Kisekka , Sharmistha Bagchi-Sen , H. Raghav Rao. "Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users" 0747-5632/$ - see front matter _ 2013 Elsevier Ltd. http://dx.doi.org/10.1016/j.chb.2013.07.023

.
.

ACKNOWLEDGMENT

First and foremost, I would like to thank Prof. S. V. Pingale for his most support and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper. Finally, I sincerely thank to my parents, family, and friends, who provide the advice and financial support. The product of this review paper would not be possible without all of them.

Prof. Subhash V. Pingale is the professor of the department of Computer science and engineering in SKN Sinhgad College of Engineering, Korti, and Pandharpur, India. His main areas of interest are Social Networks and web mining and their applications.

Mr. Sandip Shirgave born in India, in 1988. He received the B.E. degree in Computer Science & Engineering from D.K.T.E College from Shivaji University, Ichalkaranji, India, in 2012, and pursuing the Master of Engineering degrees in Computer Science & Engineering from the SKN Sinhgad College of Engineering, Korti, and Pandharpur India. His main areas of interest are Social Networks and web mining and their Applications.

ISSN: 2278 – 7798