Multi user Environment with Confidentiality Management in Online Social Networks (OSNs)

A. Sreelatha[1], Mr. S MuniKumar[2]
[1] *Student, Dept. of MCA, KMM Institute of Post Graduate Studies*
[2] *Assistant Professor, Dept. of MCA, KMM Institute of Post Graduate Studies, Tirupati,A.P*

***Abstract*- Online Social Networks (OSNs) square measure inherently designed to alter individuals to share personal and public data and build social connections with others. These OSNs provides digital social interactions and social also as personal data sharing, however in sharing variety of security and privacy issues raised. Whereas OSNs permit users to limit access to shared information, they presently don't offer any mechanism to wholly enforce privacy issue thinker related to multiple users. To the present finish, we tend to propose Associate in nursing approach to enable the protection of shared information related to multiple users in OSNs. We tend to formulate Associate in nursing access management model to capture the essence of multiparty authorization needs, in conjunction with a multiparty policy specification theme and a policy social control mechanism. Besides we tend to additionally implement a proof-of-concept prototype that is termed as MController (multi controller) having contributor, neutral and communicator controllers in conjunction with owner controller.**

***Index Terms*- social network, multipartyaccesscontrol, MController**

I. INTRODUCTION

ONLINE social networks (OSNs) such as Facebook, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family, and even with strangers. In recent years, we have seen unprecedented growth in the application of OSNs. For example, Facebook, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, and so on.) shared each month. To protect user data, access control has become a central feature of OSNs. A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and WebPages, such as wall in Facebook, where users and friends can post content and leave messages. A user profile usually includes information with respect to the user's birthday, gender, interests, education, and work history, and contact information. In addition, users can not only upload content into their own or others' spaces but also tag other users who appear in the content. Each tag is an explicit reference that links to a user's space. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationship and group membership to distinguish between trusted and untrusted users. For example, in Facebook, users can allow friends, friends of friends (FOF), groups, or public to access their data, depending on their personal authorization and privacy requirements.

Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. For instance, if a user posts a comment in a friend's space, she/he 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 concerns about the photo. To address such a critical issue, preliminary protection mechanisms have been offered by existing OSNs. For example, Facebook allows tagged users to remove the tags linked to their profiles or report violations asking Facebook managers to remove the contents that they do not want to share with the

public. However, these simple protection mechanisms suffer from several limitations. On one hand, removing a tag from a photo can only prevent other members from seeing a user's profile by means of the association link, but the user's image is still contained in the photo. Since original access control policies cannot be changed, the user's image continues to be revealed to all authorized users. On the other hand, reporting to OSNs only allows us to either keep or delete the content. Such a binary decision from OSN managers is either too loose or too restrictive, relying on the OSN's administration and requiring several people to report their request on the same content. Hence, it is essential to develop an effective and flexible access control mechanism for OSNs, accommodating the special authorization requirements coming from multiple associated users for managing the shared data collaboratively.

II. PROPOSED MODEL

MCONTROLLER

OSN is principally relationship network as well as set of users additionally as their knowledge. So OSN represented with directed labeled graph wherever every node represents user and edge denotes relationship between two users. the sting direction denotes the connection from initial to terminal node. The profile area of the user managed himself together with his privacy knowledge and content. For that privacy knowledge to keep up security many schemes are introduced. However no theme provides wholly security, principally all those schemes have just one controller that's owner. By this single controller security and privacy problems is also raised on knowledge that was personal to the owner. So that instead of the owner dominant further controller's square measure want for the versatile privacy mechanisms in OSN. the extra controllers square measure contributor, neutral and propagator which offer their own privacy policies on shared knowledge by giving the permission either allow or deny to unauthorized user on shared knowledge. Figure one illustrates totally different controllers providing their privacy policies on shared knowledge. We define multi controllers as follows:

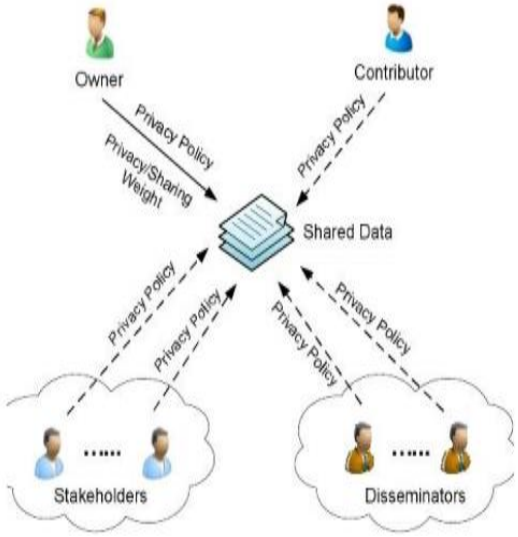

Figure.1. MController Architecture

Owner (O): within the social network the user u is termed the owner of the info item d, if d presents within the space m of user u. The user u is additionally referred to as contributor of d, once that user share knowledge item d. The owner share knowledge in 3 sorts, they're profile sharing, content sharing and relationship sharing. It allows the owner to find potential malicious activities in cooperative management.

Contributor (C): within the social network the user u is termed the contributor of the info item d, if d printed by user u in somebody else's area. The contributor tags content to other's area and also the content may additionally have multiple stakeholders (e.g., labeled users). The memory area for the user is assigned consistent with user request for content sharing.

Stakeholder (S): within the social network the user u is termed a neutral of the info item d, if user u is tagged user T for d. A shared content has multiple stakeholders.

Disseminator(D): within the social network, let d be a knowledge item shared by a user u from somebody else's area to his/her area. The user u is termed a propagator of d. the $64000 content sharing starts with the owner, then disseminator views the content

and shares with others. This disseminated content is also re-disseminated again and once more by others.

III. MULTI PARTY ACCESS CONTROL (MPAC) MODEL

MPAC Specification It is very essential for MPAC policies to regulate access and representing authorization requirements from multiple associated users to enable a collaborative authorization management of data sharing in OSNs.

ACCESSOR SPECIFICATION

Accessor is the set of users who granted to access the shared data. Accessor can be represented with a set of user names, relationship names and group names in OSNs. The accessor specification is defined as a set, accessors = {a1, a2. . . , an}, where each element is a tuple < ac,at >. where ac ∈ U ∪ RT ∪ G be a user u ∈ U, a relationship type rt ∈ RT, or a group g ∈ G. at ∈ {UN,RN,GN} be the type of the accessor specification, where UN,RN,GN represents user name, relationship name, and group name.

DATA SPECIFICATION

The data specification represented in three ways; profile, relationship and content sharing. For effective privacy the different controllers provide sensitivity levels on data. Let dt ∈ D be a data item, sl be a sensitivity level (range 0.00 to 1.00) for data item dt. The data specification is defined as a tuple < dt, sl >.

IV. MPAC POLICY

To summarize the above-mentioned specification elements, we introduce the definition of a multiparty access control policy as follows:

The multi party access control policy is a 5 - tuple

P = < controller, Ctype, accessor, data, effect > where

Controller is a user who can regulate the access of data.

Ctype is the type of the controller.

Accessor is the set of users who granted to access the shared data.

Data is represents a data specification.

Effect ∈ {permit, deny} is the authorization effect of the policy. Suppose a controller can leverage five sensitivity levels: 0.00 (none), 0.25 (low), 0.50 (medium), 0.75 (high), and 1.00 (highest) for the shared data.

V. MPAC EVALUATION

Multi party access control is evaluated in two steps. In step-1, the individual decision are collected from different controllers, and in step-2, individual decision are aggregated and makes final decision for the access request. Figure 2 illustrates that how MPAC evaluated in step by step. Initially an access request goes to under policy evaluation, which is done under four controllers. The four controllers provide their own privacy policies in the form of decision either permit or deny in step-1 process. After giving decisions by individual controllers, they are aggregated and make final decision by using decision voting schemes in step-2 process. The final decision making decides whether the access request is allowed or refused.

From the process of evaluation in MPAC policies, the controllers give different decision for an access request. There may be a chance of occurring conflicts. So that a mechanism is needed to resolute the conflicts for taking an unambiguous decision for each access request. For the better privacy, a strong resolution for conflict may need. So it is better to consider tradeoff between privacy and utility in resolution of conflict. For this conflict issue, we introduce decision voting schemes resolving the MPAC conflicts which is simple and flexible.

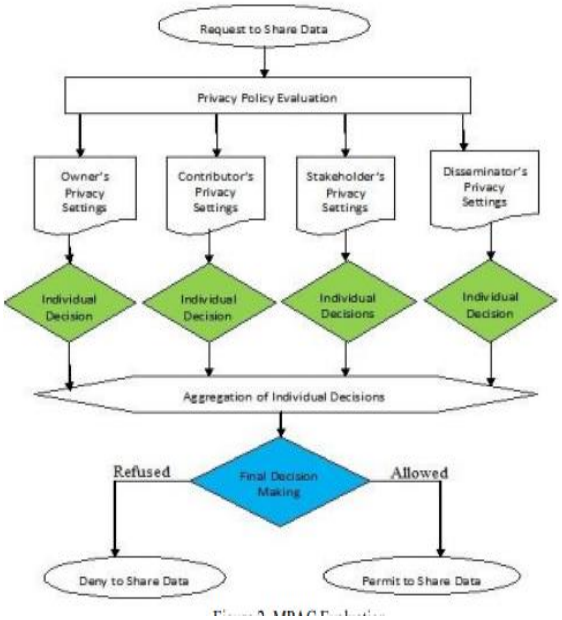

Figure.2. MPAC Evaluation

VI. CONCLUSION

In this paper, we tend to found the requirement of privacy for OSN and resolution of cooperative authorization management of the shared knowledge. We tend to introduced MController technique to supply their own privacy preferences on a shared knowledge by the various controllers. In addition MPAC model evaluated providing call vote schemes and also the privacy analysis. Within the future work, we tend to square measure attending to investigate advanced MController technique to supply privacy settings for the cluster of photos at a time, as a result of users could also be concerned to place privacy setting for the quantity of photos at a time. By this MPAC model it's time overwhelming method. So that we would study advanced MController for shared knowledge to automatic tack together the privacy.

REFERENCES

[1] B. Carminati, E. Ferrari, and A. Perego, "Rule-Based Access Control for Social Networks," Proc. Int'l Conf. On the Move to Meaningful Internet Systems, pp. 1734-1744, 2006.

[2] B. Carminati, E. Ferrari, and A. Perego, "Enforcing Access Control in Web-Based Social Networks," ACM Trans. Information and System Security, vol. 13, no. 1, pp. 1-38, 2009.

[3] E. Carrie, "Access Control Requirements for Web 2.0 Security and Privacy," Proc. Workshop Web 2.0 Security & Privacy (W2SP), 2007.

[4] J. Choi, W. De Neve, K. Plataniotis, and Y. Ro, "Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared on Online Social Networks," IEEE Trans. Multimedia, vol. 13, no. 1, pp. 14-28, Feb. 2011.

[5] J. Douceur, "The Sybil Attack," Proc. Int'l Workshop Peer-to-Peer Systems, pp. 251-260, 2002.

[6] P. Fong, "Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems," Proc. IEEE Symp. Security and Privacy (SP), pp. 263-278, 2011.

[7] P. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," Proc. First ACM Conf. Data and Application Security and Privacy, pp. 191-202, 2011.

[8] 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.

[9] J. Golbeck, "Computing and Applying Trust in Web-Based Social Networks," PhD thesis, Univ. of Maryland at College Park, College Park, MD, USA, 2005.

[10] M. Harrison, W. Ruzzo, and J. Ullman, "Protection in Operating Systems," Comm. ACM, vol. 19, no. 8, pp. 461-471, 1976.

[11] H. Hu and G. Ahn, "Enabling Verification and Conformance Testing for Access Control Model," Proc. 13th ACM Symp. Access Control Models and Technologies, pp. 195-204, 2008.

[12] H. Hu and G. Ahn, "Multiparty Authorization Framework for Data Sharing in Online Social Networks," Proc. 25th Ann. IFIP WG 11.3 Conf. Data and Applications Security and Privacy, pp. 29-43, 2011.

[13] H. Hu, G. Ahn, and K. Kulkarni, "Anomaly Discovery and Resolution in Web Access Control Policies," Proc. 16th ACM Symp. Access Control Models and Technologies, pp. 165-174, 2011.

[14] 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.

[15] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks," Proc. 27th Ann. Computer Security Applications Conf., pp. 103-112, 2011.

[16] H. Hu, G.-J. Ahn, and K. Kulkarni, "Detecting and Resolving Firewall Policy Anomalies," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 3, pp. 318-331, May 2012

[17] L. Jin, H. Takabi, and J. Joshi, "Towards Active Detection of Identity Clone Attacks on Online Social Networks," Proc. First ACM Conf. Data and Application Security and Privacy, pp. 27-38, 2011.

[18] S. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H. Choi, "D-FOAF: Distributed Identity Management with Access Rights Delegation," Proc. Asian Semantic Web Conf. (ASWC), pp. 140-154, 2006.

[19] L. Lam and C.Y. Suen, "Application of Majority Voting to Pattern Recognition: An Analysis of Its Behavior and Performance," IEEE Trans. Systems, Man and Cybernetics, Part A: Systems and Humans, vol. 27, no. 5, pp. 553-568, Sept. 1997.

[20] N. Li, J. Mitchell, and W. Winsborough, "Beyond Proof-ofCompliance: Security Analysis in Trust Management," J. ACM, vol. 52, no. 3, pp. 474-514, 2005.