INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

ACCESS CONTROL MODEL FOR SOCIAL NETWORKING SITES

Kavya .M .Menon[1], Dr.S.Uma[2]

[1] *PG Scholar,kavyamenon6@gmai.com*
[2] *professor, umakarunahind@gmail.com*
PG Scholar,PG CSE Department, Hindusthan Institute of Technology. Coimbatore,Tamil Nadu,India [1]

Head of the Department, PG CSE Department, Hindusthan Institute of Technology. Coimbatore,Tamil Nadu,India[2]

Abstract
Social networking sites have tremendous growth in recent years and it became very useful for many internet users. These Networking sites provide attractive digital social interactions and information sharing but have security and privacy issues They do not have any method to provide privacy over data with multiple users. Proposed work produce an access control model which is used for multiparty authorisation requirements .Proposed work produce logical representation for access control model

Keywords: multiparty authorisation, logical representation, social interaction, multiparty authorisation, logical representation, social interaction

1. Introduction

Usage of network and networking sites are developing rapidly in recent years. This increases the emerging of various networking sites and increased use of social networking sites like Facebook, Google +, Twitter .These social networking sites help people to share public and personal information. To protect these data and information access control became the main feature of these social networking sites. A Typical social networking site provide each user with a space contains profile information and users friends and web pages .To ensure the protection of user data, social networking sites requires users to be system and policy administrators for monitoring their data .These social networking sites use relationship and group membership to identify trusted and un trusted users.

These Social networking sites provide access control mechanism which allows users to access information contained in their spaces and they have no control on outside spaces. To address this issue a primary protection mechanism is provided by social networking sites .These simple protection mechanism has limitations .so it is essential to develop an effective access control mechanism including the special authorization requirement having multiple associated users for controlling shared data.

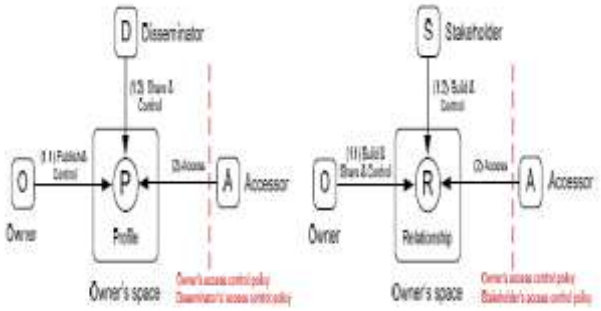
This work formulate a systematic solution to manage shared data . The work begin with the checking the lack of multiparty access control for data shared in social networking sites can insure the protection of user data. Considering these sharing patterns, a multiparty access control model is developed with features of multiparty authorization requirements that have not been considered in the existing access control system and models. The proposed model also contain multiparty policy specification scheme .A voting mechanism is provided to deal with authorization and privacy.

The compelling features of proposed model are to support analysis on the multiparty access control model and system. Thus the model is valid. Thus the use of proposed mechanism greatly enhances the flexibility for regulating sharing of data. It reduces the certainty of system authorization and privacy conflict should be minimize Access control mechanism relies on the security analysis technique is applied in various field like operating system ,trust management and role based access control. In this approach use additionally produce a method to represent and reson about this method in a logical method to represent model in logical program.

These Social networking sites provide access control mechanism which allows users to access information contained in their spaces and they have no control on outside spaces. To address this issue a priminary protection mechanism is provided by social networking sites .These simple protection mechanism have limitations .so it is essential to develop an effective access control mechanism including the special authorization requirement having multiple associated users for controlling shared data.

This work formulates a systematic solution to manage shared data. The work begin with the checking the lack of multiparty access control for data shared in social networking sites can insure the protection of user data. Considering these sharing patterns, a multiparty access control model is developed with features of multiparty authorization requirements that have not been considered in the existing access control system and models. The proposed model also contain multiparty policy specification scheme .A voting mechanism is provided to deal with authorization and privacy.

The compelling features of proposed model are to support analysis on the multiparty access control model and system. Thus the model is valid. Thus the use of proposed mechanism greatly enhances the flexibility for regulating sharing of data. It reduces the certainty of system authorization and privacy conflict should be minimize Access control mechanism relies on the security analysis technique is applied in various field like operating system ,trust management and role based access control. In this approach use additionally produce a method to represent and reson about this method in a logical method to represent model in logical program.



(a) A disseminator shares others profile (b) user shares her/his relation

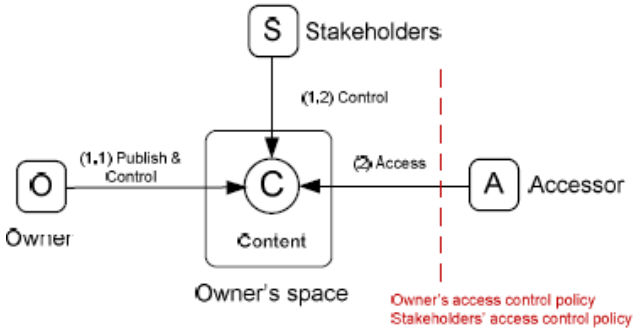
Fig.1.MPAC pattern for profile and relationship sharing

2. Profile Sharing, Content Sharing, Relationship Sharing

Profile sharing: Feature of some social networking site is to support various social applications. To provide effective and meaningful services these applications have user profile attributes like name, birthday, activities, interests etc. To make complex applications on social network platform can also consume the profile attributes of users friend. In such cases, users can choose unique pieces of profile attributes they are ready to share with applications, when the user use the application

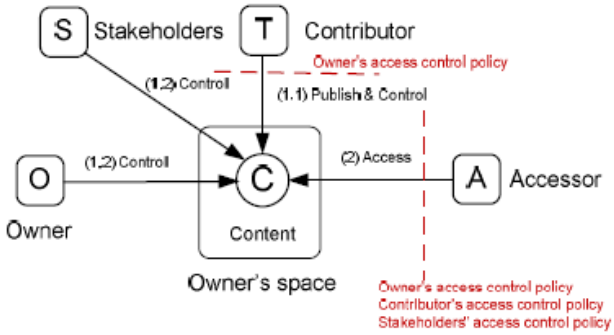
Relationship sharing: Another important feature of social network site is that users can share relationship with others. Bidirectional relationship and have potentiality sensitive information that users may not wait to make it public .Many Social networking sites provide method in which users can regulate the display of friend.

Content sharing: Social networking site provide various method that help users to communicate and share content and notes in their own space. The sharing connected with multiple users



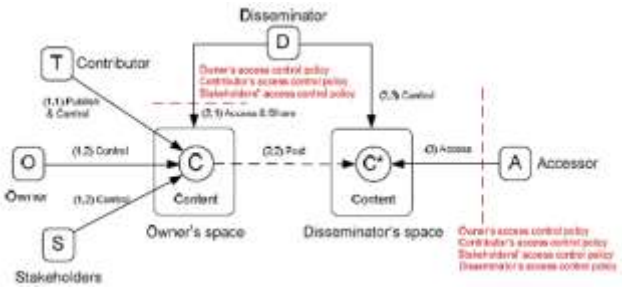
(a) A shared content has multiple stakeholders

The above figure (a) describe about profile sharing pattern in which a disseminator can share others profile attributes to an accessor.owner and disseminator can specify access control policies to restrict the sharing of profile attributes



(b) A shared content is published by a contributor

The above figure (b) shows a relationship sharing pattern where a user called owner, who has relationship with another user called stakeholder, shares the relationship with an accessor



(c) A disseminator shares others content published by a contributor

The above figure (c) shows the content sharing pattern where the sharing starts with an originator.

3. Multiparty Access Control Model

An social network site can be present by relationship network, a group and collection of user data. In relationship network of social network site is directed graph, and in which each node represent a user and edges represent relationship

between users. Each label indicated relationship and edge representation and relationship type. Edge direction represents the relationship. Edge indicates the initial node of relationship and terminal node expects relationship.

In previous years many access control models have proposed to support authorization specification of social networking sites. These models have single controller to control access control policies .A access control mechanism in a multi user environment like social network sites should be controlled by an administrator. *Their are controllers like contributors, stockholders and disseminators of data .They are defined as below.*

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.

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

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.

Disseminator: Let d be a data item shared by a user u from someone else's space to his/her space in the social network. The user u is called a disseminator of d.

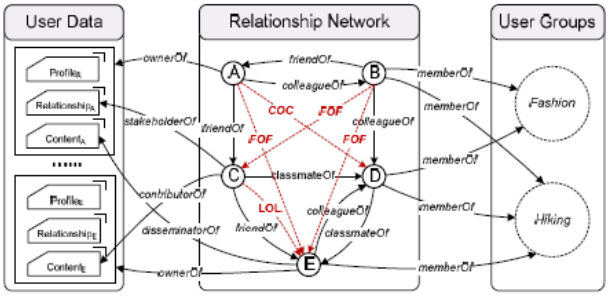


Fig 3 An example of multiparty social network representation

4. Conclusion

In proposed work a solution for collaborative management of shared data in social networking site is introduced. A Multiparty access control model is produced and along with that have policy specification scheme and also have policy evaluation. Along with that proposed model is represented and reasoned. A multiparty controller is also established in the proposed work. Future work can develop more complex privacy control scheme and better collaborative management in social networking sites.

References

1. Facebook Developers, http://developers.facebook.com/, 2013.

2. Facebook Privacy Policyhttp://www.facebook.com/policy.php/, 2013.

3. Facebook Statistics, http://www.facebook.com/press/info.php?statistics, 2013.

4 .Google+ Privacy Policy, http://http://www.google.com/intl/
en/+/policy/, 2013.

5 .The Google+ Project, https://plus.google.com, 2013.

6. G. Ahn and H. Hu, "Towards Realizing a Formal RBAC Model in Real Systems," Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 215-224, 2007.

7.G. Ahn, H. Hu, J. Lee, and Y. Meng, "Representing and Reasoning about Web Access Control Policies," Proc. IEEE 34th Ann. Computer Software and Applications Conf. (COMPSAC), pp. 137- 146, 2010.

8 .A. Besmer and H.R. Lipford, "Moving beyond Untagging: Photo Privacy in a Tagged World," Proc. 28th Int'l Conf. Human Factors in Computing Systems, pp. 1563-1572, 2010.

9. L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All Your Contacts Are Belong to Us: Automated Identity theft Attacks on Social Networks," Proc. 18th Int'l Conf. World Wide Web, pp. 551-560, 2009.

10. B. Carminati and E. Ferrari, "Collaborative Access Control in On- Line Social Networks," Proc. Seventh Int'l Conf. Collaborative Computing: Networking, Applications and Worksharing (Collaborate- Com), pp. 231-240, 2011.
11. 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. 626 IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 7, JULY 2013

12. 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.

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

14. 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.

BIOGRAPHY

Kavya M Menon

She received the B.E degree in Computer Science & Engineering from Nehru Institute of Engineering and Technology, Tamil Nadu in 2012. She is currently doing the M.E. in Computer Science and engineering in Hindustan Institute of Technology, Coimbatore, Tamil Nadu, now working on the research project in Data mining.

Dr.S.Uma is Professor and Head of the PG Department of Computer Science and Engineering at Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India. She received her B.E., degree in Computer Science and Engineering in First Class with Distinction from P.SG. College of Technology in 1991 and the M.S.,degree from Anna University, Chennai, Tamil Nadu, India. She received her Ph.D., in Computer Science and Engineering from Anna University, Chennai, Tamil Nadu, India with High Commendation. She has nearly 23 years of academic experience. She has organized many National Level events like seminars, workshops and conferences. She has published many research papers in National and International Conferences and Journals. She is a potential reviewer of International Journals and life member of the ISTE professional body. Her research interests are pattern recognition and analysis of nonlinear time series data.