ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Access Control Policies Of Socio Networking Websites For Multiple Profile Holders

B.Vijaya Kumar[1], G.Nirmala Devi[2], V.Vanaja[3], P.Meena[4]

Assistant Professor, Achariya College of Engineering Technology, Puducherry, India[1]

B.Tech-CSE Final Year, Achariya College of Engineering Technology Puducherry, India[2, 3, 4]

ABSTRACT: In recent years, online social networks (OSNs) have become an important part of daily life and become a portal for millions of Internet users. These OSNs provide attractive means for digital interactions between social network and information sharing, but also a number of security and privacy issues are increase. The online social networks also allow the user to control the shared data and presently do not provide any mechanism to enforce concerns of privacy and security over data associated with multiple users. To solve this problem, we propose a systematic approach for enabling the shared data in OSNs. An access control model is formulated to capture the essence of multiparty authorization requirements, along with a multiparty policy specification system and a policy enforcement mechanism. We begin by investigate how to control lacks for shared data in OSNs based on the relationship between the user, data and their data sharing patterns. Based on the sharing patterns, we make a Multi party Access Control (MPAC) model to control the features of multiparty authorization requirements. In our MPAC model contains a multiparty policy specification system. Also this model provides a voting mechanism to avoid conflicts.

KEYWORDS: Multi party Access Control (MPAC), online social networks (OSNs)

I. INTRODUCTION

Online social networks play a vital role in today's communication. Social networks are defined like face book, twitter, linked in, Google+ each social network have different securities measure, rules regulation and policy. Online social networks (OSNs) such as Facebook, Twitter, and Google+ are inherently designed to enable people to share personal and public information and make social connections with coworkers, family, friends, colleagues, and strangers. In facebook users can allow groups of user, friends, and even with friends of friends or public to correctly to use their data, depending on their personal authorization and privacy requirements. Although Online social networks currently provide simple access control mechanisms allowing users to govern access to information contained only in their own spaces, then the users, unfortunately, data residing outside their spaces there is no power between users. Such as, if a user posts any comment in a friend's space or friend of friend's space, He/she cannot specify which users can view the comment.

Users regularly upload personal business and education details of revealing private details to Public, to protect user information security controls have become a central feature of social networking sites but remains to users to adopt these features. Personnel data on social networks has used by employers for job searching they can communicate directly with the concern person but more sophisticated applications of social network data include tracking user behavior monitoring. Cannot trust users place in social networks exploiting with hackers and attacks, set of threats posed to users has resulted in a number of refinements to privacy controls. However one aspect of security remains largely unresolved friends photos stories and data are shared across the network conflicting privacy requirements between friends can result in information being unintentionally exposed to the public, while social networks allow users to restrict access to their own data currently no mechanism to enforce privacy concerns over data uploaded by other user social network content is made available to search engines and mined for information, personal privacy goes beyond what one user uploads about his/her becomes an issue of every member on the shares.

Access control in OSNs is typically based on the relationships among users in the social graph. That is, providing access to an accessing user is subject to the existence of a direct or indirect relationship of certain types between the accessing user and the controlling users of the target. Many existing OSN systems enforce a limited relationship-based access control mechanism, offering users the ability to choose from a pre-defined policy vocabulary, such as “public”, “private”, “friend” or “friend of friend”. Google+ and Face book recently introduced customized relationships, namely “circle” and “friend list”, providing users highly protecting options to differentiate different privileged user groups.

Multiple users can express access control policies for a user or a resource, it is expected that there will be several policies applicable to the same access request which will inevitably raise conflicts. For example, Bob sets his policy so that he can get friendship request from anyone in the system, while at the same time policies defined by his parents may only allow him to receive such request from his friends of friends. To resolve such conflicts, it is necessary to introduce conflict resolution policies, which are policies about how authorization policies are to be interpreted and how policy conflicts ate resolved.

II. EXISTING SYSTEM

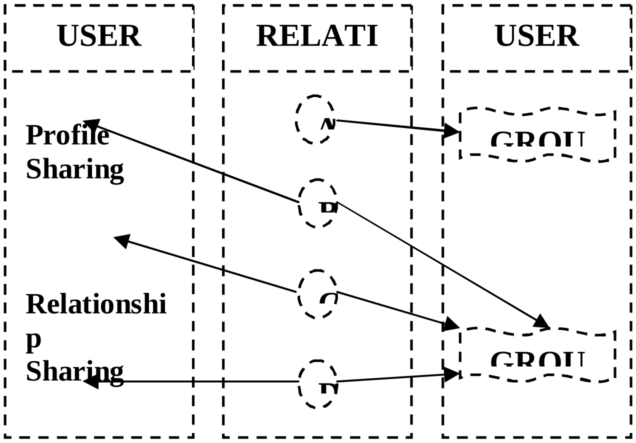
OSNs currently not provide any mechanism to enforce privacy concerns over data associated with multiple users. Model and analyze access control requirements in the existing work with respect to collaborative authorization management of shared data in OSNs. The online social network has been recognized by recent work provided a solution for collective privacy management but the need of joint management for data sharing, especially photo sharing in OSNs by multiple users. Their work considered access control policies of a content that is co-owned in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content. The shared content may be connected to the multiple stakeholders but no one can specify the access control policies. A user can only control one direction of a relationship so every user in the group can access the shared content.

III. PROPOSED SYSTEM FOR MPAC POLICIES:

In proposed system our solution is to support the analysis of multiparty access control model and mechanism systems. We implement a proof-of-concept facebook application of shared data using collaborative management approach called MController. The use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in online social networks (OSNs). Our prototype application enables multiple users to specify their privacy preferences and authorization policies to control a shared data item and current implementation was restricted to handle photo sharing in OSNs. But our approach to deal with other kinds of data sharing and post comments, the stakeholder of shared data are identified with effective methods like tagging the photo or searching the friends. The proposed system provides an effective solution of shared data in OSNs for collaborative management. The use of multiparty mechanism to enforce privacy concerns over data associated with many users and also multiparty access control model (MPAC) was formulated, along with a multiparty policy specification system and corresponding policy evaluation mechanism. In addition we have introduced an approach for representing and reasoning about our proposed model. A group of users could collude with one another so as to manipulate the final access control decision in our multiparty access control system.

IV. MODULE DESCRIPTION:

To enforced access control in online social network owner resources get in policies specification based on the interaction between two users. Edges are initial node and terminal node are accepting node. Online social network sharing data collaboration management to authorized sharing information in user side there is some modules are introduced



4.1 OWNER MODULE

In owner module let d be a data item in the space m of a user u in the social network. The contributor of d it referred from user u. We analyze three methods that is profile sharing, relationship sharing and content sharing to understand some risks posted by the lack of collaborative control in OSNs. In this owner and the disseminator can specify access control policies to restrict the sharing of profile attributes it enables the owner to discover potential malicious activities in collaborative control.

4.2 CONTRIBUTOR MODULE

In contributor module the user u is published by the data item d in someone like friend space in the social network. The user u is called the

Contributor of d. The contributor publishes content to other friend's space and also the content may be published in multiple stakeholders. In content sharing the memory space will allotted for the user according to the user request. Contributor is published by a shared content.

4.3 STAKEHOLDER MODULE

In space of user let d is a data item in the stakeholder module in the social network. Let data item d is associated set of tagged user's t. A user u is also known as stakeholder of d, if u 2 t that has a relationship with another user called stakeholder and it shares the relationship with an accessor. The authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the privacy concern stakeholder's may be violated. The content is shared among has multiple stakeholders.

4.4 DISSEMINATIOR MODULE

In Disseminator module let d be a data item and user u is shared data from someone else's space either his/her space in the social network. The user u is also called a disseminator of d. A content sharing pattern sharing starts from an originator, it publishing the content, and then a views the disseminator d and shares the content. The disseminator's friends may be further re-disseminated by a disseminated content to regulate sharing behaviors where effective access control mechanisms should be applied in each method to protect further dissemination of the content by always enforced the access control policies

4.5 MPAC MODULE

The multiparty access control model (MPAC) is used to valid proposed access control model. In MPAC model the OSNs provide a web space for each member where the store and manage the personal information. To represent authorization requirements from multiple associated users, essential for multiparty access control policies to regulate access over shared data by enable a collaborative authorization management. The proposed MPAC model our policy specification system is build. In this model used to flexible access the data and provide multiple controllers, who are associated with shared data. Accessors are a set of users who are granted
To access the shared data. Accessors can be represented with a set of user names, set of relationship names or a set of group names in OSNs.

V. CONCLUSION

In this paper, we have proposed a novel solution for privacy conflict detection and resolution for collaborative data sharing in OSNs. Formulated in MPAC model, along with multiparty policy specification scheme and policy evaluation mechanism. Also we have introduced the proof-of-concept implementation of our solution called MController along with extensive evaluation of our approach. As part of future work, we will formulate a comprehensive access control model to capture the essence of collaborative authorization requirements for data sharing in OSNs. Also we would extend our work to address security and privacy challenges for emerging information sharing services such as location sharing and other social network platforms such as Google+. In addition, users may be involved in the control of a larger number of shared photos and configurations of the privacy preferences may become time-consuming and tedious tasks.

REFERENCES

[1]FaceBookDeveleopers http://developers.facebook.com/.

[2] Facebook Privacy Policy. http://www.facebook.com/policy.php/.

[3]Facebook Statistics. http://www.facebook.com/press/info.php?statistics.

[4] Google+ Privacy Policy. http://http://www.google.com/intl/en/+/policy/.

[5] G. Ahn, H. Hu, J. Lee, and Y. Meng. Representing and reasoning about web access control policies. In Computer Software and Applications Conference (COMPSAC), 2010 IEEE 34th Annual pages 137–146. IEEE, 2010.

[6] 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.

[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]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.

[9] B. Carminati and E. Ferrari. Collaborative access control in online social networks. In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), pages 231–240. IEEE, 2011.

[10] The Google+ Project. https://plus.google.com.