International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 6, October 2014, PP 25-30
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

A Novel Model for Multiparty Access Control for Online Social Network

[1]B Surekha, [2]Dr.N Sudhakar Reddy

PG Scholar, Department of CSE, S V College of Engineering, Tirupati.
Professor, Department of CSE, S V College of Engineering, Tirupati

Abstract: *on-line social networks have practiced tremendous growth in recent years and become a factual portal for many ample web users. These on-line social networks supply enticing suggests that for digital social interactions and data sharing, however additionally move up variety of privacy and security problems. whereas on-line social networks permit users to manage access to shared knowledge, they presently don't offer any mechanism to enforce privacy concerns over knowledge related to several users. to the present finish, we have a tendency to propose associate approach to modify the protection of shared data related to multiple users in on-line social networks. we have a tendency to prepare associate access management model to require into custody the essence of multiparty authorization needs, beside a policy social control mechanism and a multiparty policy specification system. This paper we have a tendency to going study concerning model and mechanism systems in analysis of multiparty access management. The correctness of realization of associate access management model relies on the premise that the access management model is valid. pursue associate economical resolution to facilitate cooperative management of common knowledge in OSNs. we start by investigate how the dearth of multiparty access management for knowledge sharing in OSNs will undermine the protection of user knowledge. Some distinctive knowledge sharing patterns with relation to multiparty authorization in OSNs also are known. we have a tendency to build official a Multiparty Access management (MPAC) model for OSNs*

Keywords: *OSNs, access management model, multiparty authorization needs, multiparty policy specification scheme, a policy social control mechanism, Multiparty Access control (MPAC)*

1. INTRODUCTION

Online social networks (OSNs) such as Facebook, Twitter, and Google+ are essentially designed to facilitate people to share personal and public information and formulate social relations with friends, colleagues, family, and coworkers and even with strangers also. In current years, we have seen extraordinary growth in the application of OSNs. For example, Facebook, one of ambassador social network sites, claims that it has more than 900 million active users and over 35 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month. To protect user data, access control has become a central feature of OSNs. A distinctive OSN provides each user with a implicit space containing profile information, a list of the user's associates, and web pages, such as fortification in Facebook,where users and friends can place content and put down messages. A user profile usually comprises information with respect to the user's gender, birthday, education, interests, work history, and contact information. In adding together, users can not only upload content into their own or others' spaces but also attach a label to other users who become visible in the content. Every tag is an explicit reference that links to a user's space. For the protection of user data, present OSNs at one remove require users to be system and policy administrators for adaptable their data, where users can control data sharing to a specific set of trusted users. OSNs often use user connection and group membership to differentiate between trusted and untrusted users. Even though OSNs currently provide simple access control methods allowing users to administer access to information controlled in their own spaces, users, regrettably, have no control over data existing outside their spaces. For example, if a user posts a comment in a friend's space, s/he can't specify which users can view the comment. In a different case, when a user uploads an image and tags friends who become visible in the photo, the tagged friends cannot check who can observe this photo, even though the tagged friends may have dissimilar privacy concerns about the photo. To take in hand such a serious

issue, preface protection mechanisms have been offered by existing OSNs. Suppose Facebook allows tagged users to remove the tags linked to their profiles or report violations asking Facebook supervisors to remove the contents that they do not want to share with the public. These simple protection mechanisms suffer from several boundaries. On one hand, removing a tag from a photo can only avoid other members from seeing a user's profile by means of the association link, but the user's image is still enclosed in the photo. Since innovative access control policies cannot be distorted, the user's image continues to be exposed to all authorized users and reporting to OSNs only allows us to either keep or remove the content. Such a binary decision from OSN managers is either too loose or too preventive, relying on the OSN's administration and requiring several people to report their request on the same content. Therefore, it is necessary to develop an effective and flexible access control mechanism for OSNs, accepting the special authorization requirements coming from multiple associated users for managing the shared data collaboratively

2. EXISTING SYSTEM

OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no power over data residing outside their spaces. Such as, if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment. In another case, while a user uploads tags and the photograph friends who appear in the photograph, the tagged friends cannot restrict who can see this photograph, even though the tagged friends may have different privacy concerns about the photo. To address such a serious issue, beginning protection mechanisms have been offered by existing online social networks (OSNs).

- Access to a resource is granted while the requestor is able to demonstrate of being authorized.
- Every user in the group can access the shared content.
- Not give any mechanism to enforce privacy concerns over data associated with multiple users
- if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment
- while a user uploads a photo and tags friends who appear in the photograph, the tagged friends cannot restrict who can see this photograph

3. PROPOSED SYSTEM

Our solution is to support the analysis of multiparty access control model and mechanism systems. The correctness of execution of an access control model is based on the premise that the access control model is suitable. Moreover, while the use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in Online social networks (OSNs), it may potentially reduce the certainty of system authorization consequences due to the reason that authorization and privacy conflicts need to be resolved elegantly. We specially analyze the scenario like content sharing to understand the risks posted by the lack of collaborative control in online social networks (OSNs).

Proposed System Advantages

- It checks the access request against the policy specified for every user and yields a decision for the access.
- The use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in online social networks.
- present any mechanism to enforce privacy concerns over data associated with many users
- if a user posts a comment in a friend's space, he/she can specify which users can view the comment

4. MULTI PARTY ACCESS CONTROL (MPAC) MODEL:

A. 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 contentsharing. 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 >.

B. 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.

C. 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 4 illustrates that how MPAC evaluated in step by step. Initially an accessvrequest 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.

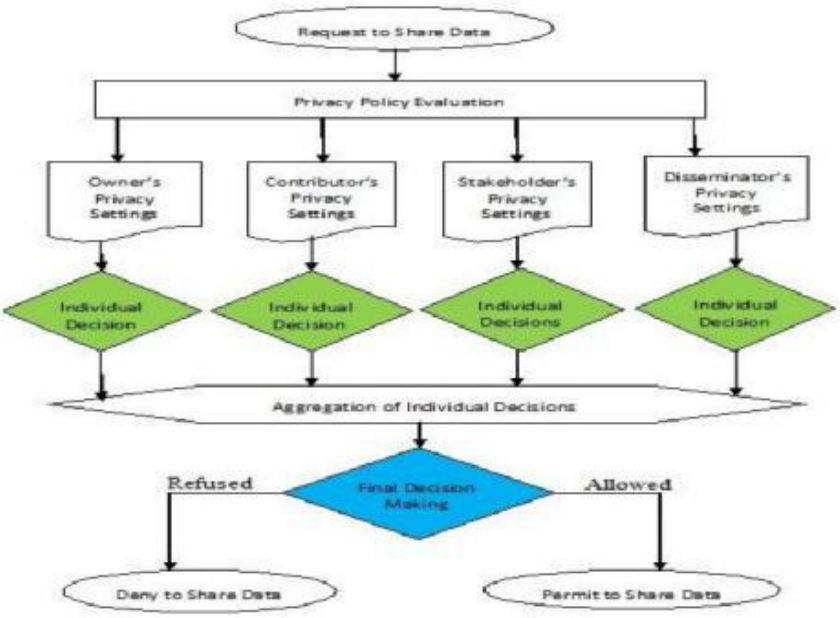

Figure.4. *MPAC Evaluation*

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.

5. METHODOLOGIES

A methodology is the process of acquiring communication traces in large scale parallel application.

Modules Name: Authentication (login /Registration), Profile, Friends, Send request, Group, Photos

Authentication (login /Registration)

Fig.

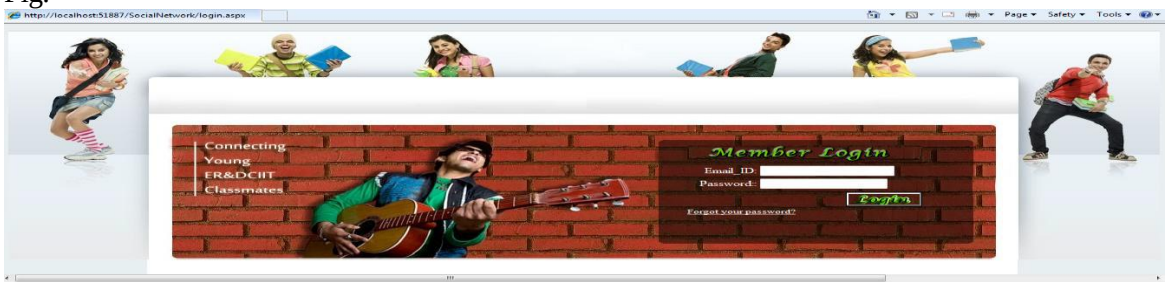

Fig. 1 *Example of an Authentication*

Home

Fig. 2 *Example of Home*

Profile

In this module user make our profile that details store in database the profile contains name, contact no, and email address, photos, and other information. Logged users can see their details and if they wish to change any of their information they can edit it.

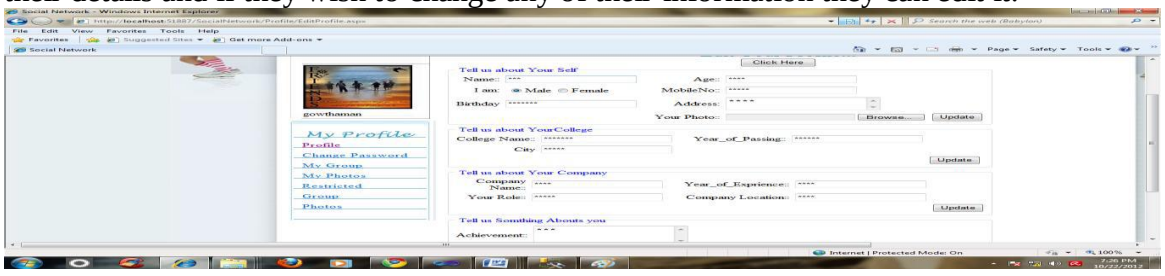

Fig. 3 *Example of Profile*

Groups

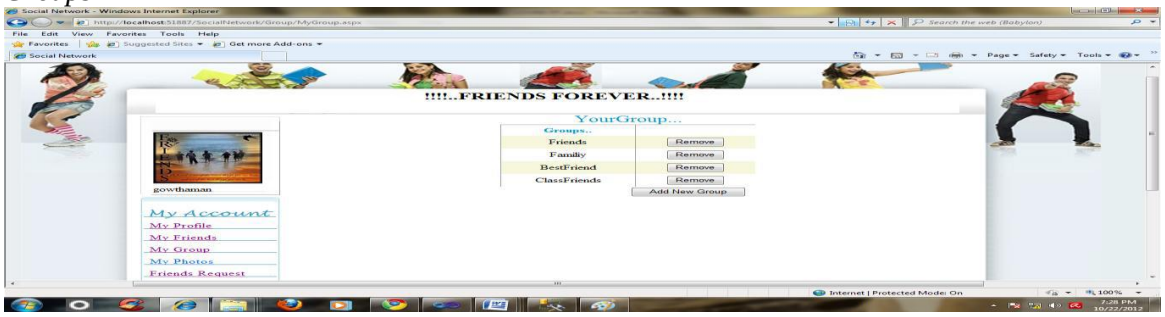

Fig. 4 *Example of Groups*

Friend Request

In this module user select friend to send request. logged user view request accept our friend request

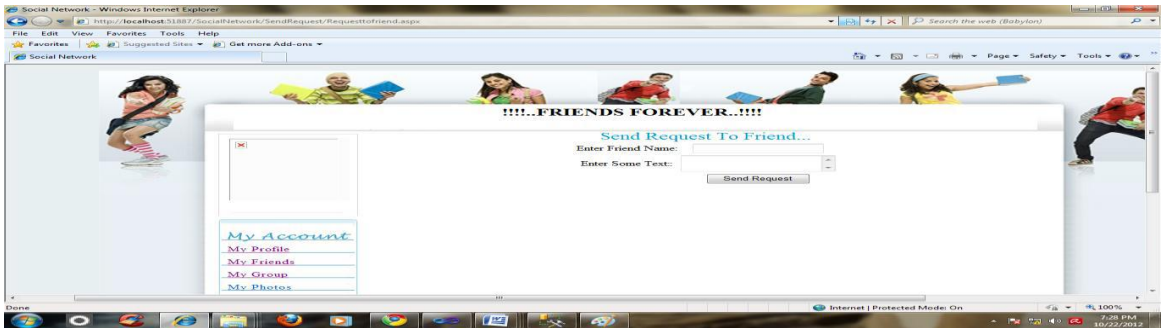

Fig. 4 *Example of Friend Request*

Photos

In this module user add new photo and publish the content based on our selected members in that group. Who appear in the photo, the tagged friends can restrict who can see this photo if (user = = Allow) that User will be allowed to access the data's Else User will be not allowed to access the data's This module enables the user to upload the photos to their photo gallery and maintain their album

6. CONCLUSION

In our multiparty access control system for model and mechanism, a group of users could collude with one another so as to manipulate the final access control decision. An attack scenarios, anywhere a set of malicious users may want to make a shared photo available to a wider audience. Suppose they can access the photo, and then they all tag themselves or fake their identities to the photo. In addition, they collude with each other to assign a very low sensitivity level for the photo and specify policies to grant a wider audience to access the photo with a large number of colluding users, the photo may be disclosed to those users who are not expected to gain the access. To prevent such an attack scenario from occurring, three conditions need to be satisfied: (1) there is no fake identity in OSNs; (2) all tagged users are real users appeared in the photo; and (3) all controllers of the photo are honest to specify their privacy preferences.

REFERENCES

[1]. 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.

[2]. E. Carrie. Access Control Requirements for Web 2.0 Security and Privacy. In *Proc. Of Workshop on Web 2.0 Security & Privacy (W2SP)*. Citeseer, 2007.

[3]. 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. *Multimedia, IEEE Transactions on*, 13(1):14–28, 2011.

[4]. P. Fong. Relationship-based access control: Protection model and policy language. In *Proceedings of the first ACM conference on Data and application security and privacy*, pages 191–202. ACM, 2011.

[5]. J. Golbeck. Computing and applying trust in web-based social networks. Ph.D. thesis, University of Maryland at College Park College Park, MD, USA. 2005.

[6]. H. Hu and G. Ahn. Multiparty authorization framework for data sharing in online social networks. In *Proceedings of the 25th annual IFIP WG 11.3 conference on Data and applications security and privacy*, pages 29–43. Springer-Verlag, 2011.

[7]. H. Hu, G. Ahn, and K. Kulkarni. Anomaly discovery and resolution in web access control policies. In *Proceedings of the 16th ACM symposium on Access control models and technologies*, pages 165– 174. ACM, 2011.

[8]. B. Viswanath, A. Post, K. Gummadi, and A. Mislove. An analysis of social network- based sybil defenses. In *ACM SIGCOMM Computer Communication Review*, volume 40, pages 363–374. ACM, 2010.

[9]. G. Wondracek, T. Holz, E. Kirda, and C. Kruegel. A practical attack to de-anonymize social network users. In *2010 IEEE Symposium on Security and Privacy*, pages 223–238. IEEE, 2010.

[10]. E. Zheleva and L. Getoor. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th international conference on World Wide Web*, pages 531–540. ACM, 2009.