# User Access Control for OSNs: An Empirical Study in the Offing

**Saritha Bhukya**[1]
sarimothi@gmail.com

**Usha Gayatri** [2]
ushagayatri@gmail.com

**K Chandra Sekharaiah**[3]
chandra_sekharaiah@yahoo.com

***Abstract: Online Social networking has been described as the contemporary way that people interact. OSN facilitates people to share personal and public information and make social connections with others. (Online Social networks have become an integral part of online lives)OSNs are a great way to stay connected with others, but it also raises a number of security and privacy issues. Whereas OSNs allow users to control access to shared data, at the moment they do not provide any mechanism to implement privacy concerns over data connected with multiple users. While online social networks allow users to control access to shared data, they presently do not provide any mechanism to enforce privacy concerns over data associated with many users. The proposed approach is to assist the security of shared data associated with many users in OSNs. We put together an access control replica to capture the fundamental nature of multiparty agreement requirements, along with a multiparty strategy requirement scheme and a policy enforcement mechanism. Here we present a logical demonstration of our access control model which allows user to control the features of presented logic solvers to execute various analysis tasks on our model. We introduced a proof-of-concept prototype of our move toward as part of an application in Face book and make available usability study and system valuation of our method.***

***Keywords: Social network, multiparty access control, security model, policy specification and management***

# 1. Introduction

An Online social network plays a important role in today's interpersonal communication. Examples of social networks are Facebook, twitter, linked in, Google+ and etc. Each social network has differed with respect to security measure rules and regulation and policy. Mainly security for user is not up to the mark. In face book if a person wants to share a data or images or video or audio to friend if user share that video it is publicly available in social network. And everyone see it even if he shares only with his friends if his friend likes it then it is to all the friends in his list can see it. So privacy and security is not there. In time line there is no security for cover photos. In this if we add security question for everything shared by applying member ship criteria like friend, family etc. then if his friend wants to see it he must give security answer for the question. And user cannot share it, this can be very helpful in providing user level security. In this Facebook must add this security tag for user security in sharing information. By using access control policies & question tags we can provide secure communication in online social networks. Online social networks (OSNs) such as Face book, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, co-workers, colleagues, family and even with strangers. In recent years, we have seen have 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,

[1] The first author is in the 4th semester of M.Tech (CNIS) in School Of Information Technology JNTUH, India and is a project student with the 3rd author.
[2] The 2nd author is an Assistant Professor in MVSR College of Engineering, Hyderabad, India and is a Ph.D. scholar with the 3rd author.
[3] The 3rd author is a Professor in CSE, School of IT, JNTUH.

 

photo albums, etc.) 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 provide profile information, a list of the user's friends, and web pages, such as wall paper in Facebook, where users and friends can post content and leave messages. And user profile usually includes information with respect to the user's birthday, gender, interest's education and work history, and contact information. In addition, users can not only upload content into their own or others' spaces butt 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 us membership to distinguish between trusted and untrusted users. For example, in Face book, users can allow friends, friends of friends, groups or public to access their data, depending on their personal authorization and privacy requirements.

The rest of the paper is organized as follows. Section 2 gives background and motivation scenario for the work. Section 3 presents the related work. Section 4 concludes the paper.

# 2. Background and Motivation

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, co-workers, 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, etc.) 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 web pages, 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, 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, user 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. In

 

this paper, we pursue a systematic solution to facilitate collaborative management of shared data in OSNs. We begin by examining how the lack of multiparty access control for data sharing in OSNs can undermine the protection of user data. Some typical data sharing patterns with respect to multiparty authorization in OSNs are also identified. Based on these sharing patterns, a multiparty access control (MPAC) model is formulated to capture the core features of multiparty authorization requirements which have not been accommodated so far by existing access control systems and models for OSNs. Our model also contains a multiparty policy specification scheme. Meanwhile, since conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in our model. Another compelling feature of our solution is the support of analysis on multiparty access control model and systems. The correctness of implementation of an access control model is based on the premise that the access control model is valid. Moreover, while the use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in 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. Assessing the implications of access control mechanisms traditionally relies on the security analysis technique, which has been applied in several domains (e.g., operating systems, trust management, and role-based access control). In our approach, we additionally introduce a method to represent and reason about our model in a logic program. In addition, we provide a prototype implementation of our authorization mechanism in the context of Facebook. Our experimental results demonstrate the feasibility and usability of our approach.

# 3. Related Work

**Analysis of Problem:**

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, s/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, Face- book allows tagged users to remove the tags linked to their profiles or report violations asking Face- book 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.

**Proposed Work and Objectives:**

The survey study has given us cues to propose to implement a proof-of-concept Facebook application for the collaborative management of shared data. We call it MController. Our prototype application will enable multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. Our implementation will be restricted to handling photo sharing in OSNs. Obversely, our approach can be generalized to deal with other kinds of data sharing and comments, in OSNs as long as the stakeholder of shared data are identified with effective methods like tagging or searching. The proposed system will give a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model. A proof-

 

of-concept implementation of our solution called MController has been discussed as well, followed by the usability study and system evaluation of our method. Indeed, a flexible access control mechanism in a multi-user environment like OSNs should allow multiple controllers, who are associated with the shared data, to specify access control policies. As we identified previously in the sharing patterns in addition to the owner of data, other controllers, including the contributor, stakeholder and disseminator of data, need to regulate the access of the shared data as well. In our multiparty access control system, a group of users could collude with one another so as to manipulate the final access control decision.

**Scope & Objectives:**

Online Social Networks (OSNs) are platforms that allow people to publish details about themselves and to connect to other members of the network through links. Recently, the popularity of OSNs is increasing significantly. For example, Facebook now claims to have more than a hundred million active users. The existence of OSNs that include person specific information creates both interesting opportunities and challenges. For example, social network data could be used for marketing products to the right customers. At the same time, security and privacy concerns can prevent such efforts in practice. Improving the OSN access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. However, most of current OSNs implement very basic access control systems, by simply making a user able to decide which personal information are accessible by other members by marking a given item as public, private, or accessible by their direct contacts. In order to give more flexibility, some online social networks enforce variants of these settings, but the principle is the same.

**Objectives:**

a. security policies
b. un authorized access control
c. Provide policy and privacy for multiple user to specify there authorization
d. Discover potential malicious activities using collaborative control
e. An Online Social Network with User Defined Privacy

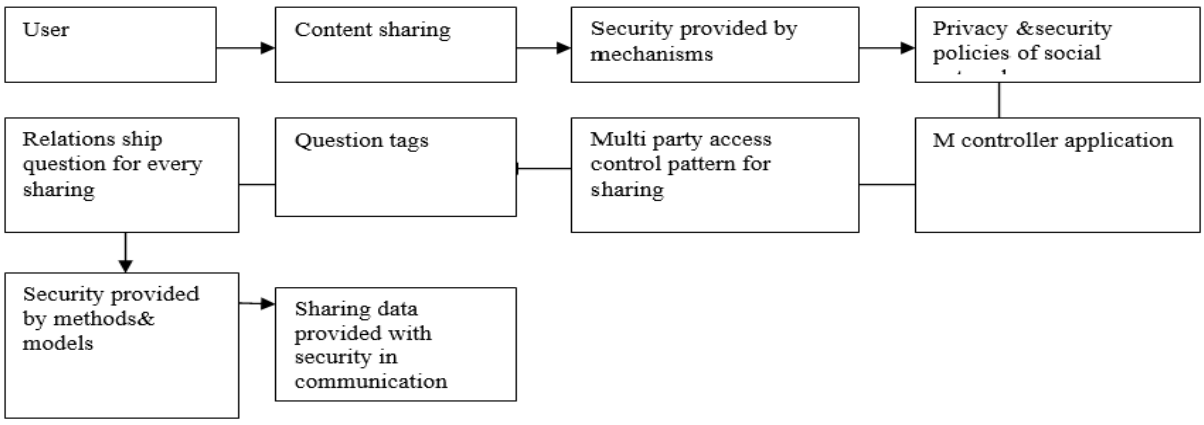


**Figure: Realtime Execution Approach for Secure Sharing of Data in OSNs**

**Theoretical explanation of background process of security in data sharing in OSNs:**

First use login to user account then if he/she share data like images, videos then security mechanisms like privacy &security policies of social network comes into act then MPAC controller module application plays a key role then we apply new concept of question tags for every sharing and seeing the post after answering the question then the content is displayed this is how we provide security in online social networks for content sharing.

 

# 4. Conclusions and Future Work

In this paper, we have conducted a survey study w.r.t. collaborative management of shared data in OSNs, user access control model along with multiparty policy specification schemes and corresponding policy evaluation mechanisms. The study helps us to introduce an approach for representing and reasoning about our proposed model for OSNs. A proof-of-concept implementation of our solution called MController is in the offing, followed by the usability study and system evaluation of our method. As part of future work, we are planning to investigate more comprehensive privacy conflict resolution approach and analysis services for collaborative management of shared data in OSNs. Also, we would explore more criteria to evaluate the features of our proposed MPAC model. For example, one of our recent works has evaluated the effectiveness of MPAC conflict resolution approach based on the trade-off of privacy risk and sharing loss. In addition, users may be involved in the control of a larger number of shared photos and the configurations of the privacy preferences may become time- consuming and tedious. Towards future work, we would study inference-based techniques, for automatically configuring privacy preferences in MPAC model.

**References:**

**[**1**]** Face book Developers. http://developers.facebook.com/.
**[**2**]** Face book Privacy Policy. http://www.facebook.com/policy.php/.
**[**3**]** Andrew Besmer and Heather Richter Lipford, "Moving Beyond Untagging:Photo Privacy in a Tagged World", In Proceedings of the ACM SIGCHI International Conference on Human Factors in Computing System, 10-15 April 2010, Atlanta, GA, USA, pp.1563-1572
**[**4**]** Barbara Canninati and Elena Ferrari, "Collaborative Access Control in Online Social Networks", In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Orlando, Florida, USA, October 15-18, 2011, pp.231-240.
**[**5**]** Jae Young Choi, Wesley De Neve, and Konstantinos N. Plataniotis "Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections", IEEE Transactions on Multimedia, Vol. 13, No. 1, February 2011, pp.14-28.
[6] A. D. Miller and W. K. Edwards. Give and take: A study of consumer photo-sharing culture and practice. In Proceedings of the SIGCHI conference on Human factors in computing systems, pages 347–356, San Jose, California, USA, 2007. ACM.
[7]. J. Palank. Face it: Book no secret to employers – The Washington Post, July 2006.
[8]. L. Palen and P. Dourish. Unpacking "privacy" for a networked world. In Proceedings of the SIGCHI conference on Human factors in computing systems,pages 129–136, Ft. Lauderdale, Florida, USA, 2003.ACM.
[9]. A. Romano. Walking a new beat: Surfing MySpace.com helps cops crack the case. - Newsweek, Apr. 2006.
[10]. Z. Stone, T. Zickler, and T. Darrell. Autotagging facebook: Social network context improves photo annotation. In Computer Vision and Pattern Recognition Workshops, 2008. CVPRW '08. IEEE Computer Society Conference on, pages 1–8, 2008.
[11]. K. Strater and H. R. Lipford. Strategies and struggles with privacy in an online social networking community. In Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People and Computers XXII: Culture, Creativity, Interaction - Volume 1, pages 111–119, Liverpool, United Kingdom, 2008. British Computer Society.
[12]. K. W. Thomas. Conflict and conflict management Reflections and update. Journal of Org
[13] S. Yan, D. Xu, B. Zhang, H. J. Zhang, Q. Yang, and S. Lin, "Graph embedding and extensions: A general framework for dimensionality reduction," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 1, pp.40–51, 2007.
[14] J. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "Face recognition using kernel direct discriminant analysis algorithms," *IEEE Trans Neural Netw.*, vol. 14, no. 1, pp. 117–126, 2003.
[15] B. Moghaddam, T. Jebara, and A. Pentland, "Bayesian face recognition," *Pattern Recognit.*, vol. 33, no. 11, pp. 1771–1782, 2000.

 

[16] P. N. Belhumeur, J. P. Hesphanha, and D. J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection,"
*IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 9, no. 7, pp. 711–720, 1997.
[17] M. A. Turk and A. P. Pentland, "Eigenfaces for recognition," *J. Cognitive Neurosci.*, vol. 3, no. 1, pp. 71–86, 1991.
[18] V. Perlibakas, "Distance measures for PCA-based face recognition," *Pattern Recognit. Lett.*, vol. 25, no. 12, pp. 1421–1430, 2004.
[19] L. Chen, B. Hu, L. Zhang, M. Li, and H. J. Zhang, "Face annotation for family photo album management," *Int. J. Image Graph.*, vol. 3, no. 1, pp. 1–14, 2003.
[20] J. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "Regularized discriminant analysis for the small sample size problem in face
recognition," *Pattern Recognit. Lett.*, vol. 24, no. 16, pp. 3079–3087, 2003.
[21] A. Vlachou, C. Doulkeridis, D. Mavroeidis, and M.Varzirgiannis, "Designing a peer-to-peer architecture for distributed image retrieval," in *Proc. LNCS Int. Conf. Adaptive Multimedia Retrieval: Retrieval, User, and Semantics*, 2008.
[22] M. Bender, T. Crecelius, and M. Kacimi, "Peer-to-peer information search: Semantic, social, or spiritual?," *IEEE Data Eng. Bull.*, vol. 30, no. 2, pp. 51–60, 2008.
[23] J. Lu and K. N. Plataniotis, "On conversion from color to gray-scale images for face detection," in *Proc. IEEE Int. Conf. Computer Vision and Pattern Recognition Workshops*, 2009.
[24] C. M. Bishop, *Pattern Recognition and Machine Learning*. Berlin, Germany: Springer, 2006 .

 