International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-3, February 2014

A Novel Approach Of MPAC Model For Online Social Network

J. Lydia Jeba, R. Nandhini

Abstract— Online Social Networks (OSNs) have increased and become a concerning fact for billions of internet users like Facebook, Twitter, My space, etc. In OSNs the shared data are restricted by the user and currently for the multiple users they do not provide any mechanism. To overcome this issue we propose a model for the multiple users of shared data in OSNs. For multiparty authorization, policy specification scheme and policy enforcement mechanism we formulate an access control model to capture the essence of multiparty.

Index term— Multiparty access control, Authorization, Policy specification and Management.

I. INTRODUCTION

Online social networks (OSNs) such as Facebook, Twitter, My Space is used to share their information with family, friends and even with strangers. We have seen an extraordinary growth in recent years. OSNs give straight forward access management techniques to regulate users to access information contained in their own wall. Users do not have any management of information existing outside their wall.

The OSNs central feature is access management. We have a tendency to pursue a scientific answer to facilitate cooperative management of shared knowledge in OSNs. Therefore, we propose a Multiparty authorization framework (MAF) and Multiparty access control (MPAC) model in OSNs. We begin by examining how the multipath access control model for shared knowledge in OSNs will undermine the protection of user knowledge. A multiparty authorization model is developed to capture the core options of multiparty authorization needs that are not accommodated by existing access management systems.

MPAC model manipulates user to access final control decision. Normally the user has more control over his/her photos. When the user accesses their photo from original user, they tag photos with fake identities and further share with other users also. By this process the original photo may change totally, then can be shared with a number of users.

The privacy of the photo which was expected by original user may collude totally. To control this we have to identify fake users and all tagged users in OSNs.

Manuscript published on 28 February 2014.
***** Correspondence Author (s)
J.Lydia Jeba*, Computer Science and Engineering,Sathyabama University, Chennai,India.
R.Nandhini, Computer Science and Engineering,Sathyabama University, Chennai,India.

II. RELATED ARTICLES

Choi et al. (2011) introduced a conceptually-similar but more comprehensive trust-based access control model. This model allows the specification of access rules for online resources, and the authorized persons are denoted in the form of the relationship type and trust level between users in OSNs. They further presented a semi-decentralized discretionary access control model and a related enforcement mechanism for controlling the sharing of information in OSNs. Fong et al. (2011) formulated the paradigm called a Relationship Based Access Control model. None of these existing works could model and analyze access control requirement. An access control model that formalizes and generalizes the access control mechanism implemented in Facebook based on theoretical graph properties that admits arbitrary policy vocabularies.

Qureshi et al. (2010) a novel solution shows the proposed system for collaborative management of shared data in online social network. Generalized approach is used to identify the data shared in different kinds of OSNs and the stakeholder identifies the shared data by tagging or searching OSNs, which are proved to be effective. Multiparty access control model along with policy evaluation mechanism has been formulated.

Ahn et al. (2010) multi-user access control has been developed to secure network and existing access control solutions, for trust based access control and reputation in OSNs. In based ontology distributed identity management the relationships are based on the trust level, which indicates the level of friendship between the users and the relationship with the user. The specification rules for online resource denotes the authorized users. Semi-decentralized model is formulated.

Wondracek et al. (2010) to exploit group membership information and group member relationship, a novel de-anonymization attack is used. Group membership is identified by web browser, stealing attacks. To involve de-anonymization attack the user visits malicious website and the visitors are identified by both theoretical analysis and empirical measurements. A normal sized social network is mainly used to explore larger social networks and used for business related in OSNs.

Aruna et al. (2013) to improve security and privacy the users actually demand the complete access control mechanisms that are not achieved by the social networks. The individual users can select different problems causing privacy conflicts in shared data with multiple users. Proof-of-concept prototype is discussed in a solution called “MC controller” has been followed by system evaluation method and usability studies.

Rachel et al. (2013) the need for privacy and solution for the shared data in collaborative authorization management are identified and MC controller techniques. Users introduced privacy on shared data are provided by different controllers.An MC controller's advanced technique for privacy settings are implemented for group photos. These techniques are used automatically to organize privacy preferences in MPAC model. In MPAC model the notion of trust and reputation are systematically integrated and the solution of comprehensive copes with collusion attacks are investigated for providing service for robust MPAC in OSNs.

III. EXISTING SYSTEM

In OSNs simple access control mechanism is currently provided to access information. Unfortunately, users have no control over information outside their spaces. In this issue a preliminary protection mechanism is offered by online social networks. They have several limitations for the simple protection mechanism. By association link the removed photo of the tag can be viewed by other visitors from user's profile with user image still visible on the friend's profile. Another main issue in OSNs is to identify the fake user. For, example in twitter the person will have multiple number of profiles with the same user name that are created by strangers or fake user. The fake user can access the photo and can tag to a large number of colluding users, thus exposing the photo to fake users.

IV. PROPOSED WORK

In collaborative management of shared data in OSNs a systematic solution has been implemented to facilitate management. The proposed work starts by finding the lack of multiparty access control (MPAC) for sharing the data with multiple users that can compromise the protection of user data in OSNs. By some typical sharing patterns the multiparty authorization is identified in OSNs. MPAC model is formulated to capture the core of multiparty authorization requirements by sharing the patterns. In the available system this authorization requirement has not been implemented. By trust level, the user may identify the fake user. A multiparty policy specification scheme is also implemented in this model.

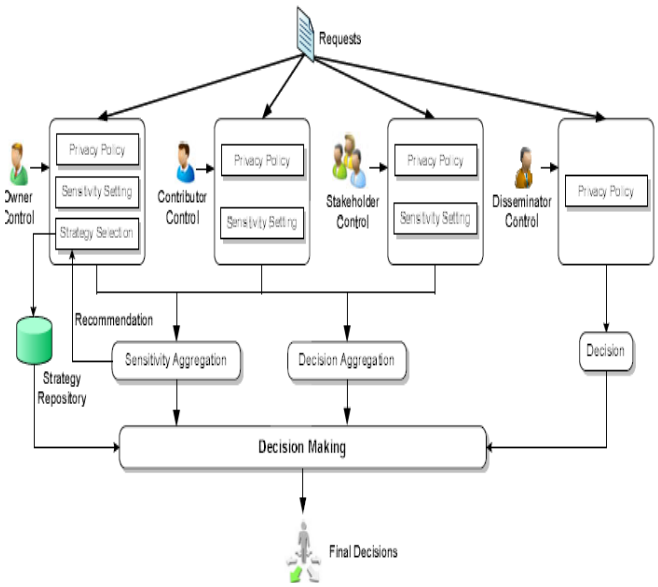

Figure 1:Architecture diagram

The MC controller is a component of the decision making model. It contains owner control, contributor control, stakeholder and disseminate control. For decision making MC Controller is used to access policies on request and evaluates the request and response to that controller that are aggregated to final decision. The policy strategy controllers are used to evaluate decision policy controller. In selection strategy the aggregated score sensitivity is defined as the recommendation process. By combining the disseminator's decision and the original controller decision the final decision is formulated.

V. CONCLUSION

The proposed technique for collaborative organization of shared data is a novel solution in OSNs, providing as a multiparty access control model along with policy scheme and policy assessment mechanism. The features of our proposed MPAC model is formulated to identify the fake identities in OSNs. A multiparty policy specification scheme and corresponding policy evaluation mechanism are accompanied by access control model.

REFERENCES

[1] J. Choi, W. De Neve, K. Plataniotis, and Y. Rio. 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.

[2] 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.

[3] B. Qureshi, G. Min, and D. Kouvatsos. Collusion detection and prevention with fire+ trust and reputation model. In Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, pages 2548–2555. IEEE, 2010.

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

[5] G. Wondracek, T. Holz, E. Kirda, and C. Kruegel. A practical attack to die anonymous social network users. In 2010 IEEE Symposium on Security and Privacy, pages 223–238. IEEE, 2010.

[6] Ch. Aruna, G. Mine, International Journal of Modern Engineering Research (IJMER) Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2808-2812.

[7] A. k. Rachel Praveena, B. Dr. S. Durga Bhavani,C.k.Suresh Babu,International journal of computer science & Network Solutions December.2013-Volume 1. No4 ISSN 2345-3397.