Multiuser access control for online social networks: by using of multiparty access control

A.M.Prashanth Kumar M. Tech (C.S.E), CREC, JNTUA, Tirupati, India
Associate Professor, J. Ravi Kumar M. Tech (C.S.E), CREC, JNTUA, Tirupati, India

ABSTRACT:

Now a day Online social networks (OSNs) have got an exponential growth and become a fame to millions of Internet users. These OSNs offer attractive ways and methods for social interactions and information sharing. Also OSNs allow users to restrict access to shared data but it is not effective in enforcing security over the data. In this paper , we propose an approach to provide the protection by considering multiparty authorization requirements. It also explained a logical representation of our access control model that allows us to leverage the features of existing logic solvers to perform various analysis tasks on our model.

Key words- Social Network, Digital social interaction, Privacy Policy, Multiuser authorization.

INTRODUCTION

Social networks (OSNs) are designed to enable people to share personal and public information and make social connections with friends, well known persons, colleagues, family and even with outsider. In early years, we have seen unprecedented growth in the application of social networks. 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, videos, etc.) shared every month. To protect user data or information, access control has become a central feature of OSNs. A typical OSN provides each user with a virtual space containing profile data, a list of user’s friends, and web pages, such as wall in Facebook, where users and friends can post content and leave normal messages. A user profile usually includes information (like phone number ) with respect to the user’s birthday, gender, interests, education, photo’s and work history, and contact details. In additionally in this system, users can not only upload a content into their own or others’ spaces but also tag other users who appear in the content. For each tag is an explicit reference that links to a user’s space. For the safeguard of user data, the current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can hold down data sharing to a specific set of trusted users.

EXISTING SYSTEM:

The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data or content in OSNs. The needfulness of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs. In their work considered access control policies of a content that is co-owned by multiple user’s in an Online social networks, such that each co-owner may separately specify her/his own privacy preference for the shared content.

DISADVANTAGES OF EXISTING SYSTEM:

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 send or post a comment in a friend’s space, she/he cannot specify which users can view the comment.

PROPOSED SYSTEM:

In this paper, we pursue a systematic solution to facilitate collaborative management of shared data or content in OSNs. We begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user
data. Some typical content or data sharing patterns with respect to multiparty authorization in OSNs are also identified. Based on these sharing patterns, a multiparty access control model is formulated to capture the core features of multiparty authorization requirements that have not been accommodated so far by existing access control systems and models for OSNs.

ADVANTAGES OF PROPOSED SYSTEM:

Regulate access over the shared data, representing the authorization requirements from multiple associated users. A proof-of-concept implementation of our solution called MController has been discussed as already, followed by the usability study and system evaluation of our method. Actually, a flexible access control mechanism in a multi-user environment like OSNs should allow multiple controllers, who are associated with the shared content or data, to specify the access control policies. As we find out 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 current system multiparty access control system, a group of users could with one another so as to manipulate the final access control decision.

SYSTEM ARCHITECTURE:-

MODULES:-

After careful analysis the system has been identified to have the following modules:

1. Owner Module
2. Contributor Module
3. Stakeholder Module
4. Disseminator Module
5. MPAC Module

MODULES DESCRIPTION:

1. Owner Module:-

In Owner module let \( d \) be a data item in the space \( m \) of a user \( u \) in social networks. In this system user \( u \) is called the owner of \( d \) and the user \( u \) is called the contributor of \( d \). As we specifically analyze three scenarios—profile sharing, relationship sharing, details sharing and content sharing—to understand the risks posted by the lack of collaborative control in OSNs. In this model the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes (ex: user names or values). Thus, it enables the owner to discover potential malicious activities in collaborative control. The detection of collusion behaviors in collaborative systems has been addressed by the recent work.

2. Contributor Module:-

In Contributor module let \( d \) be a data item published by a user \( u \) in someone else’s space in social networks. The contributor publishes content to other’s space and the content may also have multiple stakeholders (e.g., tagged users). The memory space for the user will be allotted according to user request for content sharing. A shared content is published by a contributor.

3. Stakeholder Module:-

In Stakeholder module let \( d \) be a data item in the space of a user in the social networks. Let \( T \) be the set of tagged users associated with \( d \). Here user \( u \) is called a stakeholder of \( d \), if \( u \in T \) who has a relationship with another user called accessor. In this module, authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the stakeholder’s privacy concern may be violated. A shared content has multiple stakeholders.

4. Disseminator Module: -
In Disseminator module let d be a data item shared by a user u from someone else’s space to his/her space in the social networks. Here the user u is called a disseminator of d. The content sharing pattern where the sharing starts with an originator (owner or contributor who uploads the content) publishing the content, and then a disseminator views and shares the content. All access control policies defined by associated users should be enforced to regulate access of the content in disseminator’s space. For a more complicated case, the disseminated content may be further re-disseminated by disseminator’s friends, where effective access control mechanisms should be applied in each procedure to regulate sharing behaviors. Especially, regardless of how many steps the content has been re-disseminated, the real access control policies should be always enforced to protect further dissemination of the content.

5. MPAC Module:

MPAC is used to prove if our proposed access control model is valid. To enable a collaborative authorization management of data sharing in OSNs, it is essential for multiparty access control policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users.

Our policy specification scheme is built upon the proposed MPAC model. Accessor Specification: Accessors are a set of users who are granted to access the shared data. Accessors can be represented with a set of user names, asset of relationship names or a set of group names in OSNs.

CONCLUSION

Multiparty access control for online social network has proposed 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 extension, we have introduced an approach for representing and reasoning about our proposed model. A proof-of-concept implementation of current solution called MController has been discussed as well, followed by the usability study of the system and system evaluation of our current system method.

FUTURE WORK

As part of the future work, we are planning to investigate more comprehensive privacy conflict resolution approach and analysis services for collaborative management of shared data in OSNs.

REFERENCES:
IEEE, 2011.
ACM, 2011.


A.M. Prasanth Kumar received his B. Tech degree from the department of Information Technology; Sraswathi Velu College Of Engineering (Affiliated to ANNA UNIVERSITY CHENNAI). He is pursuing M.Tech in Computer Science Engineering from Chadalawada Ramanamma Engineering College (Affiliated to JNTU ANANTAPUR), Tirupati, AP, India. His current research interests are Data Mining.

J. Ravi Kumar M.Tech (C.S.E) Associate Professor in Chadalawada Ramanamma Engineering College (CREC) Affiliated by JNTU Anantapur in Tirupati, A.P area of interest is Data Mining and Network Security