Multi Party Authorization Framework for Data Sharing in Online Social Networks

ARJUNAGARI YUGANDHA1, ORVAKANTI DEVAKIRAN2

1PG Scholar, Dept of CSE, Shree Institute of Technical Education, Tirupati, AP, India, Email: kalvapushpa438@gmail.com.
2Asst Prof, Dept of CSE, Shree Institute of Technical Education, Tirupati, AP, India, Email: odevakiran@gmail.com.

Abstract: Online Social Networks (OSNs) are essentially designed to facilitate people to share personal and public information and make social connections with others. These OSNs propose good looking means for digital social communications and information distribution, but also raise 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. The proposed approach is to facilitate the defense of shared data associated with many users in OSNs. We put together an access control replica to capture the essence of multiparty agreement requirements, along with a multiparty strategy requirement scheme and a policy enforcement mechanism. Here present a logical demonstration of our access control model which allows us to influence 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 Facebook and make available usability study and system valuation of our method. The survival of OSNs that include person detailed information creates attractive openings for various applications ranging from advertising to group of people organization. Security and privacy concerns need to be dealt with for creating such applications. Improving social network access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. To address some of the current limitations, we have created an experimental social network using synthetic data which we then use to test the efficacy of the semantic reasoning based approaches we have previously suggested.

Keywords: Security Model, Social Network, Multiparty Access Control, Policy Specification and Management.

I. 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.

Figure 1. Multiparty Access Control Pattern for Profile and Relationship Sharing

We instigate by examining how the lack of multiparty access control for data sharing in OSNs can weaken the protection of user data. Some distinctive data sharing prototypes with respect to multiparty approval in OSNs are also identified. Based on these distribution patterns, a multiparty access control (MPAC) model is put together to capture the core features of multiparty authorization requirements which have not been contained so far by existing access control systems and models for OSNs. Proposed model also contains a multiparty policy specification scheme. In the meantime, since conflicts are predictable in multiparty authorization enforcement, a voting mechanism is additional provided to deal with authorization and privacy conflicts in this model

II. RELATED WORK

Multi user access control is introduced for secure network access, existing access control solutions for online social networks trust based access control inspired by the developments of trust and reputation in online social networks. The friend of friend ontology based distributed identity management system for online social network where relationships are associated with a trust level which indicates the level of friendship between the users participating in a given relationship. This model allows the specification access rules for online resource where authorized users are denoted in terms of the relationship type depth and trust level between user’s in online social networks. Semi-decentralized discretionary access control model and a related enforcement mechanism for controlled sharing of information in online social network. Fong et al proposed an access control mechanism in Facebook admitting arbitrary policy vocabularies that are based on theoretical graph properties described relationship based access control as one of new security paradigms that addresses unique requirements of Web 2.0 then Fong (Ahn, 2010) (Ahn, 2007) recently formulated this paradigm called a relationship based access control model that bases authorization decisions on the relationship between the resource owner and the resource access or in an online.

The data sharing specialty photo sharing in online social network Squicciarini et al provided a solution for collective privacy management in online social networks. Their work considered access control policies of a content that is co-owned by multiple users in online social networks such that each co-owner may separately specify his or her own privacy preference for the shared content. Carminati et al. (Choi et al, 2011) (Hu et al, 2011) recently introduced a new class of security policies, called collaborative security policies that basically enhance topology-based access control with respect to a set of collaborative users. In contrast, our work proposes a formal model to address the multiparty access control issue in OSNs, along with a general policy specification scheme and a simple but flexible conflict resolution mechanism for collaborative management of shared data in OSNs. In particular, our proposed solution can also conduct various analysis tasks on access control mechanisms used. (Hu et al, 2011) (Hu et al, 2012)

III. PROBLEM DEFINITION

An online social network provides the conversation on different activities such as business education entertainment advertisement etc. attractive means of digital social interactions raise the number of security concerns associated with multiple online users. The access control captures a multiuser authorization requirement which provides the privacy issue. For example frequently used social network Facebook user only accepts his/her friends but all are in different domains, to share information on same domain need to accepts the profiles of unauthorized users trigger security and privacy issue our system provides multi access control to share relation, profile & information. Profile sharing feature is to support social applications written by external party developers to build functionalities of user profiles. Relationship sharing is that users can share their relationship with other members inherently bidirectional and carry potential sensitive information that associated users may not need to disclose. Content sharing provide built in mechanisms enabling users to communicate and share contents with other members.

Figure 2. Proposed Multiuser Access Control Mechanism
Multi Party Authorization Framework for Data Sharing in Online Social Networks

A. M Controller

OSN is mainly relationship network including set of users as well as their data. So that OSN represented with directed labeled graph where each node represents user and edge denotes relationship between two users. The edge direction denotes the relationship from initial to terminal node. The profile space of the user managed himself with his privacy data and content. For that privacy data to maintain security several schemes are introduced. But no scheme gives totally security, mainly all those schemes have only one controller that is owner. By this single controller security and privacy issues may be raised on data which was personal to the owner.

![Figure 3. M controller Architecture.](image)

So that rather than the owner controlling additional controllers are need for the flexible privacy mechanisms in OSN. The additional controllers are contributor, stakeholder and disseminator which provide their own privacy policies on shared data by giving the permission either permit or deny to unauthorized user on shared data. Figure 3 illustrates different controllers providing their privacy policies on shared data. We define multi controllers as follows:

1. Owner (O)
   
   In the social network the user u is called the owner of the data item d, if d presents in the space m of user u. The user u is also called as contributor of d, when that user share data item The owner share data in three types, they are profile sharing, content sharing and relationship sharing. It enables the owner to discover potential malicious activities in collaborative control.

2. Contributor (C)
   
   In the social network the user u is called the contributor of the data item d, if d published by user u in someone else’s space. The contributor tags 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.

3. Stakeholder (S)
   
   In the social network the user u is called a stakeholder of the data item d, if user u is tagged user T for d. A shared content has multiple stakeholders.

4. Disseminator (D)
   
   In the social network, let d be a data item shared by a user u from someone else’s space to his/her space. The user u is called a disseminator of d. the real content sharing starts with the owner, then disseminator views the content and shares with others. This disseminated content may be re-disseminated again and again by others.

B. Multi Party Access Control (MPAC) Model

1. 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 ac ∈ 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 content sharing. 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 >.

2. 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

   \[ P = < \text{controller}, \text{Ctype}, \text{accessor}, \text{data}, \text{effect} > \]

   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 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.

3. 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 access request 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.

**IV. EXPERIMENTAL RESULT**

**Figure.5.Home Page.**

**Figure.6.New Users.**

**Figure.7. Multiparty Sharing.**

**Figure.7. Multiparty Result.**
V. 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. 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.

VI. REFERENCES