Model and Mechanisms in Relationship-based Access Control for Online Social Network

S. Khadervalli,II[nd] Sri Sai Institute of Technology And Science, Rayachoti, Kadapa.

M.Atheequllah Khan, Associate Professor Sri Sai Institute of Technology And Science, Rayachoti, Kadapa.

***Abstract*—User-to-user (U2U) relationship-based access control has become the most prevalent approach for modeling access control in online social networks (OSNs), where authorization is typically made by tracking the existence of a U2U relationship of particular type and/or depth between the accessing user and the resource owner. However, today's OSN applications allow various user activities that cannot be controlled by using U2U relationships alone. In this paper, we develop a relationship-based access control model for OSNs that incorporates not only U2U relationships but also user-to-resource (U2R) and resource-to-resource (R2R) relationships. Furthermore, while most access control proposals for OSNs only focus on controlling users' normal usage activities, our model also captures controls on users' administrative activities. Authorization policies are defined in terms of patterns of relationship paths on social graph and the hopcount limits of these path. The proposed policy specification language features hopcount skipping of resource-related relationships, allowing more flexibility and expressive power. We also provide simple specifications of conflict resolution policies to resolve possible conflicts among authorization policies This paper we going study about model and mechanism systems in analysis of multiparty access control. The correctness of realization of an access control model is based on the premise that the access control model is valid...We pursue an efficient solution to facilitate collaborative management of common data in OSNs. We begin by investigate how the lack of multiparty access control for data sharing in OSNs can undermine the protection of user data. Some distinctive data sharing patterns with respect to multiparty authorization in OSNs are also identified. We make official a Multiparty Access Control (MPAC) model for OSNs.**

I. INTRODUCTION

Online social networks (OSNs) have attracted a large amount of users to regularly connect, interact and share information with each other for different purposes. Users share a tremendous amount of content with other users in OSNs using various services. The explosive growth of sensitive or private user data that are readily available in OSNs has raised an urgent expectation for effective access control that can protect these data from unauthorized users in OSNs.

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

In OSN, users are allowed to configure access control policies for their own content and activities. Allowing U2R relationship-based access control further enables users to spec-ify policies for contents related to them and activities of other related users. Since a change of relationships may result in a change of authorization, the creation and termination of relationships needs to be treated differently from usage activities to normal resources. Thus, access control in OSNs has to address the management of access control policies and relationships in addition to normal usage activities by means of U2U, U2R and R2R relationships. Although Carminati et al [6], [7] introduced a framework that allows system admin-istrators to specify administrative policies in ontology-based representations, they did not provide a policy management model for managing policies and resolving policy conflicts. Most of the other relationship-based access control models do not incorporate users' administrative activities.

Since multiple users can express access control policies for a user or a resource, it is expected that there will be several policies applicable to the same access request which will inevitably raise conflicts. For example, Bob sets his policy so that he can get friendship request from anyone in the system, while at the same time policies defined by his parents may only allow him to receive such request from his friends of friends. To resolve such conflicts, it is necessary to introduce conflict resolution policies, which are (meta-)policies about how authorization policies are to be interpreted and how policy conflicts are resolved.

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

II. Related Works

In Proposed System we implemented a proof-of-concept Facebook application for the collaborative management of shared data, called MController. Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. It is worth noting that our current implementation was restricted to handle 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 shows 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.

B. Modules

Owner Module

In Owner module let d be a data item in the space m of a user u in the social network. The user u is called the owner of d. The user u is called the contributor of d. We specifically analyze three scenarios—profile sharing, relationship sharing and content sharing—to understand the risks posted by the lack of collaborative control in OSNs. In this the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. 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.

The Owner performs activities like:

- Register & login
- Find friends
- Uploads images
- Views friends page
- Hides/Unhide relationship

Contributor Module

In Contributor module let d be a data item published by a user u in someone else's space in the social network. 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

The Contributor performs activities like:

•Publishes content in others space.

Stakeholder Module

In Stakeholder module let d be a data item in the space of a user in the social network. Let T be the set of tagged users associated with d. A user u is called a stakeholder of d, if user wants a relationship with another user called stakeholder, shares the relationship with an accessor. In this scenario, 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.

The StakeHolder performs activities like:

- Participates in voting for uploading an image, where he/she is tagged.

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 network. The user u is called a disseminator of d. A 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 original access control policies should be always enforced to protect further dissemination of the content.

The Disseminator performs activities like:

- Shares content with owner's permission

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, a set of relationship names or a set of group names in OSNs.

III.WEB ACCESS CONTROL POLICIES

A. Representing and Reasoning

We propose a systematic method to represent XACML policies in answer set programming (JSP), a declarative programming paradigm oriented towards combinatorial search problems and knowledge intensive applications. Compared to a few existing approaches to formalizing XACML policies. our formal representation is more straightforward and can cover more XACML features. Furthermore, translating XACML to JSP allows us to leverage off-the-shelf JSP solvers for a variety of analysis services such as policy verification, comparison and querying. In addition, in order to support *reasoning* about role-based authorization constraints, we introduce a general specification scheme for RBAC constraints along with a policy analysis framework, which facilitates the analysis of constraint violations in XACML-based RBAC policies. The expressivity of ASP, such as ability to handle default reasoning and represent transitive closure, helps manage XACML and RBAC constraints that cannot be handled in other logic-based approaches . We also overview our tool XACML2ASP and conduct experiments with real-world XACML policies to evaluate the effectiveness and efficient of our solution

B.Requirements for Apache Tomcat Security and Privacy

The increased social networking capabilities provided by Apache Tomcat technologies requires a examination of what we consider "private" and what we consider "personal" information, and will consequently drive a new way of limiting and monitoring the information that we make public online. Tomcat Server --applications are creating large, composite conglomerations of personal data and so we need new approaches to describe and execute access organize on that data. "Private" information at present tends to be insecurely defined by legislation, rather than by what individuals consider to be personal. Generic information such as a person's home address and phone number are normally considered personally identical information (PII) and are to be protected when collected and stored by an organization in addition, the use and release of exact data, such as medical or financial information, is restricted legislatively. However, It also exists information that an individual may consider to be personal, and want to let loose only to people meeting particular criteria (such as people attending the same school) or particular people (such as close friends). Thus someone might want to control portions of their digital life in the same manner that they control what information is released in their analog life. In the world, a person can choose to tell someone or some group some piece of information about themselves. On the other hand, it is often the case that in the online world these controls do not exist, most important to de facto public disclosure.

IV ONLINE SOCIAL NETWORKS

A.Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared on Online

Social Networks

We propose a novel collaborative face recognition frame work, improving the accuracy of face annotation by effectively making use of multiple face recognition engines available in online social networks. Our collaborative face
recognition framework consists of two major parts: merging (or fusion) and selection of face recognition engines of multiple face recognition results. The selection of face recognition engines aims at determining a set of modified face recognition engines that are suitable for recognizing query face images belonging to a particular member of the Online social networks. For this purpose, we use both social network context in an online social networks and social context in personal photograph collections. In addition, to take advantage of the availability of multiple face recognition results retrieved from the selected face recognition engines, we devise two effective solutions for merging face recognition results, adopting traditional techniques for combining multiple classifier outputs. Experiments were conducted using 547 991 personal photographs collected from an existing Online social networks. Our results demonstrate that the proposed collaborative face recognition method is able to significantly improve the accuracy of face annotation, compared to conventional face recognition approaches that only make use of a single face recognition engine. Further, we demonstrate that our collaborative face recognition framework has a low computational cost and comes with a design that is suited for deployment in a decentralized online social network.

Protection model and policy language:

Social Network Systems pioneer a paradigm of access control that is distinct from traditional approaches to access control. The Gates coined the term Relationship-Based Access Control (ReBAC) to refer to this paradigm. Relationship-Based Access Control is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships. This work explores what it takes to widen the applicability of Relationship-Based Access Control to

application domains other than social computing. We prepare an archetypical Relationship-Based Access Control model to capture the essence of the standard, that is, authorization decisions are based on the relationship between the resource owner and the resource accessor in a social network maintained by the security system. A novelty of the model is that it captures the contextual nature of associations. We work out a policy language, based on modal logic, for composing access control policies that support delegation of trust. We use a case study in the domain of Electronic Health Records to demonstrate the utility of our model and its policy language. This provides initial evidence to the feasibility and utility of Relationship-Based Access Control as a general-purpose paradigm of access control.

Multiparty Authorization Framework for Data Sharing and An Active Detection of Identity Clone Attacks

We propose a multiparty authorization framework (MAF) to model and realize multiparty access control in online social networks. We begin by examining how the lack of multiparty access control for data sharing in online social networks can undermine the security of user data. A multiparty authorization model is then 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 online social networks. In Meanwhile, as conflicts are inevitable in multiparty authorization specification and enforcement, systematic conflict resolution mechanism is also addressed to cope with authorization and privacy conflicts in our framework. We first examine and characterize the behaviors of ICAs. Then we propose a detection framework that is focused on discovering suspicious identities and then validating them. Towards detecting suspicious identities, we propose two approaches based on attribute similarity and similarity of friend networks.

MPAC Model:

OSN can be represented by a relationship network. OSNs provide each member a Web space where users can store and manage their personal data including profile information, friend list and content. 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. We identified previously in the sharing patterns, in addition to the other controllers, owner of data including the stakeholder, contributor and disseminator of data, need to regulate the access of the shared data as well We define these controllers as follows:

Definition 1: (Owner). Let **d** be a data item in the space of a user **u** in the social network. The user **u** is called the owner of **d**.

Definition 2: (Contributor). Let **d** be a data item published by a user **u** in someone else's space in the social network.The user **u** is called the contributor of **d.Definition 3: (Stakeholder).** Let **d** be a data item in the space of a user in the social network. Let **T** be the set of taggedusers associated with **d**. A user **u** is called a stakeholder of **d**, if **u** ∈**T** .**Definition 4: (Disseminator).** Let **d** be a data item shared by a user **u** from someone else's space to his/her space in thesocial network. The user **u** is called a disseminator of **d.**MPAC Policy Specification:

The MPAC policies

(1) "Alice authorizes her friends to view her status identified by status01 with a medium sensitivity level, where Alice is the owner of the status."
(2) "Bob authorizes users who are his colleagues or in hiking group to view a photo, summer.jpg, that he is tagged in with a high sensitivity level, where Bob is a stakeholder of the photo."
(3) "Carol disallows Dave and Edward to watch a Image, that she uploads to someone else's spaces with a highest sensitivity level, where Carol is the contributor of the Image." are expressed as:

(1) p1 = (Alice,OW, {< friendOf,RN >},< status01, 0.50 >, permit)
(2) p2 = (Bob, ST, {< colleageOf,RN >,< hiking,GN >},< summer.jpg, 0.75 >, permit)
(3) p3 = (Carol,CB, {< Dave,UN >,< Edward,UN >},< play.avi, 1.00 >, deny)

V 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

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.

VI FUTURE ENHANCEMENT

We define security to the application where the data which is being shared by the owner in the wall of the friends profile is restricted to share in his wall based on the sharing policy defined by the owner.

VII. 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] L. Backstrom, P. Boldi, M. Rosa, J. Ugander, and S. Vigna. Four degrees of separation. *CoRR*, abs/1111.4570, 2011.

[2] S. Benferhat, R. El Baida, and F. Cuppens. A stratification-based approach for handling conflicts in access control. In *Proceedings of the eighth ACM symposium on Access control models and technologies*, SACMAT '03, pages 189–195, New York, NY, USA, 2003. ACM.

[3] E. Bertino, S. Jajodia, and P. Samarati. Supporting multiple access control policies in database systems. *ACM Transactions on Database Systems*, 26:2001, 1996.

[4] E. Bertino, S. Jajodia, and P. Samarati. A flexible authorization mechanism for relational data management systems. *ACM Trans. Inf. Syst.*, 17(2):101–140, Apr. 1999.

[5] E. Bertino, P. Samarati, and S. Jajodia. Authorizations in relational database management systems. In *Proceedings of the 1st ACM confer-ence on Computer and communications security*, CCS '93, pages 130– 139, New York, NY, USA, 1993. ACM.

[6] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thu-raisingham. A semantic web based framework for social network access control. In *Proceedings of the 14th ACM symposium on Access control models and technologies*, SACMAT '09, pages 177–186, New York, NY, USA, 2009. ACM.

[7] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thurais-ingham. Semantic web-based social network access control. *Computers and Security*, 30(2C3):108 – 115, 2011. Special Issue on Access Control Methods and Technologies.

[8] G. Ahn, H. Hu, J. Lee, and Y. Meng. Representing and reasoning about web access control policies. In *Computer Software and ApplicationsConference (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 sharedon online social networks. *Multimedia, IEEE Transactions on*, 13(1):14–28, 2011.

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

BIOGRAPHY

S.KHADER VALLI Completed B.Tech from Madina Engineering College, Kadapa and pursuing M.Tech student of the department of Computer science and engineering in Sri Sai Institute of Technology And Science, Rayachoti, Kadapa., His main areas of interest are Social Networks and web mining and other related applications.

M.ATHEEQULLAH KHAN ,ASSO PROF, HOD CSE DEPT., received in Sri Sai Institute of Technology And Science, Rayachoti, Kadapa and M.Tech [CSE] from J.N.T.U, Hyderabad, in 2011.