IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 7, Jul 2014, 163-168

MULTIPARTY ACCESS CONTROL MECHANISM FOR ONLINE SOCIAL NETWORKS

AVINASH V NAIR[1] & SWAPNA HARI[2]

[1]Research Scholar, Department of Computer Science & Engineering, Marian Engineering College, Trivandrum, Kerala, India

[2]Associate Professor, Department of Computer Science & Engineering, Marian Engineering College, Trivandrum, Kerala, India

ABSTRACT

In recent years we have been watching a tremendous increase in the growth of online social networks(OSNs). OSNs enable people to share personal and public information and make social connections with friends, family members and other peoples. In addition to the rapid increase in the use of social network, it raises a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to totally enforce privacy issue solver associated with multiple users. The proposed method implements a solution yo facilitate collaborative management of common data item in OSNs. Each controller of the data item can set his privacy settings to the shared data item. The proposed method also identifies privacy conflicting segments and helps in resolving the privacy conflicts and a final decision is made whether or not to provide access to the shared data item.

KEYWORDS: Online Social Networks, Multiparty Access control, Policy Specification, Privacy Conflicts

INTRODUCTION

Many people are interested in sharing personal and public information about them and make social connections with friends, coworkers, colleagues, family and even with strangers through the help of online social networks (OSNs) such as Facebook, Google+, and Twitter. In recent years, we have seen the tremendous growth in the application of OSNs. OSN provides each user with a virtual space containing profile information, a list of the user's friends, as wall in Facebook, where friends and users can post data, contents, statuses and leave messages. A user profile contains information with respect to the user's birthday, gender, likes, education and work history, and contact information. Users can upload contents into their or others profile and can tag users who appear in the content. A tag is a reference to others profile or user space. OSNs allow the users to be policy administrators or the protection of user data [3]. Users can restrict data sharing to a set of trusted people.

Even though OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, have no control over data residing outside their spaces. Simple protection mechanisms have been provided by the OSN eg: removing a tag from the photo. But these mechanisms suffer certain limitations. For example removing a tag simply removes the name tag from the photo, but the photo still remains there. Hence it is necessary to develop an access control mechanism including all the authorization requirements from multiple users. Each of the controllers of the content can set his/her privacy settings and can specify who can see the content. If two users disagree on whom the shared data is to be exposed, then privacy conflict occurs. So a mechanism is required to identify the privacy conflicting segments and resolve those privacy conflicts.

RELATED WORK

Existing access control mechanisms for online social networks [1] are based on the trust and reputation. 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. Based on the relationship type, depth and trust level between the users in online social network, this model allows the specification access rules for online resource. Social Network Systems pioneer a paradigm of access control that is distinct from traditional approaches to access control. Gates coined the term Relationship-Based Access Control (ReBAC)[4] to refer to this paradigm. ReBAC is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships. Another work demonstrates that in Facebook-style Social Network Systems (FSNSs)[2], which are a generalization of the access control model of Facebook, an access control policy specifies a graph-theoretic relationship between the resource owner and resource accessor that must hold in the social graph in order for access to be granted. The paper named Rule-Based Access Control for Social Networks [6] presented an access control model for WBSNs, where policies are specified in terms of constraints on the type, depth, and trust level of relationships existing between users. Relevant features of our model are the use of certificates for granting relationships' authenticity, and the client-side enforcement of access control according to a rule-based approach, where a subject requesting to access an object must demonstrate that it has the rights of doing that by means of a proof. In contrast to the existing methods, the new method proposes a model to capture 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.

MULTIPARTY ACCESS CONTROL MODEL FOR OSN

OSN is represented by a friendship network, a set of user groups and a collection of user data. The friendship network of an OSN is a graph, where a user is represented by a node and each edge represents a friendship link between two users. OSNs include an important feature called groups where users can be organized in it where each group has a unique name. Group enables users of an OSN to easily find other users with whom they might share specific interests. Figure 1 shows the system architecture of the proposed system.

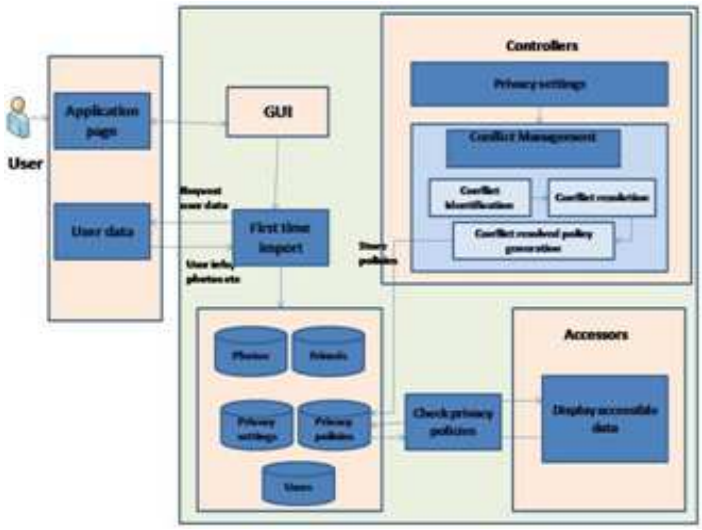

Figure 1: System Architecture

Privacy Policy Specification

Privacy requirements from multiple associated users over the shared data item are essential for the collaborative management of data sharing in OSNs. Multiple users can set their privacy requirements over the shared data item.

Controller Specification

In addition to the owner of a data item, the other controllers include contributor, disseminator and stakeholders also need to control the use of shared data.

Owner: In Owner module 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*.

Contributor: 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).

Stakeholder: 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 *u* $\in$ *T* who has 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.

Disseminator: 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

Accessor Specification

Accessors are a set of users to who are granted access to the data. Accessors can be represented with a set of user names, the friendship or a set of group names in OSNs. To Employ collaborative privacy management, trust level is introduced which is assigned to the accessors while defining privacy policies.

Data Specification

User data is made up of three components. *User profile* describes who a user is in the OSN. *User friendship* shows who a user knows in the OSN, including a list of friends to represent connections with family, coworkers etc. *User content* indicates what a user has in the OSN, including photos, videos, statues, and all other data items. Let d $\in$ D be a data item, and sl be a sensitivity level, which is a rational number in the range [0, 1], assigned to d. The data specification is defined as a tuple < d; sl >.

Privacy Policy

A privacy policy is a 4-tuple P = < controller; accessor; data; effect >, where controller is a controller specification, accessor is an access specification, data is a data specification and effect $\in$ {permit; deny} is the authorization effect of the policy.

Identifying and Resolving Privacy Conflicts

A privacy conflict occurs when two users disagree on whom the shared data item should be exposed to. The main reason leading to the privacy conflicts is that multiple associated users of the shared data item have different privacy concerns over the data item. For example, assume that Carol and David are two controllers of a photo. Each of them defines a privacy policy stating only her/his friends can view this photo. It is so impossible that Alice and Bob have the same set of friends, privacy conflicts may always exist considering collaborative control over the shared data item. The primitive solution for this problem is to allow the common friends of both parties to access the data. But this solution doesn't always produce desirable results for resolving multiparty privacy conflicts. A strong conflict resolution strategy may provide a better privacy protection. In the meantime, it may reduce the social value of data sharing in OSNs. Therefore, it is important to consider the trade-off between privacy protection and data sharing while resolving privacy conflicts. To address this problem, a mechanism for identifying multiparty privacy conflicts, as well as a systematic solution for resolving multiparty privacy conflicts is introduced.

Privacy Conflict Identification

By specifying the privacy policies to reflect the privacy concern, a set of trusted users who can access the data item is defined by each controller of the shared data item d. The set of trusted users represents an accessor space for the controller. Then we segment the accessor space of all accessors into disjoint segments as conflicting segments and non conflicting segments. A conflicting segment doesn't contain all controllers access spaces that means some of the accessors are untrusted by some controllers. A non conflicting segment covers all the accessors spaces that means all the accessors are trusted by all the controllers.

Privacy Conflict Resolution

The process of privacy conflict resolution makes a decision to allow or deny the accessors within the conflicting segments to access the shared data item. Allowing the assessors contained in conflicting segments to access the data item may cause privacy risk, but denying a set of accessors in conflicting segments to access the data item may result in sharing loss. The proposed privacy conflict resolution approach attempts to find an optimal tradeoff between privacy protection and data sharing.

Measuring Privacy Risk: The privacy risk of a conflicting segment is an indicator of potential threat to the privacy of controllers in terms of the shared data item. Higher the privacy risk of a conflicting segment, the higher the threat to controllers' privacy.

The privacy risk of a conflicting segment is calculated by a monotonically increasing function with the following parameters:

- **Number of Privacy Conflicts:** The number of privacy conflicts in a conflicting segment is indicated by the number of the untrusting controllers denoted by controllersut(i)..
- **General Privacy Concern of an Untrusting Controller*:*** The general privacy concern of an untrusting controller j is denoted as pcj. The general privacy concern of a controller can be derived from her/his default privacy setting for data sharing.

- **Sensitivity of the Data Item:** Data sensitivity in a way defines controllers' perceptions of the confidentiality of the data being transmitted. The sensitivity level of the shared data item explicitly chosen by an untrusting controller j is denoted as sl_j
- **Visibility of the Data Item:** The visibility of the data item with respect to a conflicting segment captures how many accessors are contained in the segment.
- **Trust of an Accessor:** The trust level of an accessor k is denoted as tl_k, which is an average value of the trust levels defined by the trusting controllers of the conflicting segment for the accessor.

The privacy risk of a conflict segment i due to an untrusting controller j, denoted as PR(i, j), is defined as

$$PR(i, j) = pcj \otimes slj \otimes \sum k \in accessors(i) \otimes (1 - tlk) \quad (1)$$

where, function accessors(i) returns all accessors in a segment i, and ⊗ operator is used to represent any arbitrary combination functions. For simplicity, we utilize the product operator.

In order to measure the overall privacy risk of a conflicting segment i, denoted as PR(i), we can use following equation to aggregate the privacy risks of i due to different untrusting controllers.

$$PR(i) = \sum j \in controllersut(i) (PR(i, j))$$

$$= \sum j \in controllersut(i) (pcj \times slj \times \sum k \in accessors(i) (1 - tlk)) \quad (2)$$

Measuring Sharing Loss: When the decision of privacy conflict resolution for a conflicting segment is "deny", it may cause losses in potential data sharing, since there are controllers expecting to allow the accessors in the conflicting segment to access the data item. Similar to the measurement of the privacy risk, five factors are adopted to measure the sharing loss for a conflicting segment. Compared with the factors used for quantifying the privacy risk, the only difference is that we will utilize a factor, number of trusting controllers, to replace the factor, number of privacy conflicts (untrusting controllers), for evaluating the sharing loss of a conflicting segment. The overall sharing loss SL(i) of a conflicting segment i is computed as follows:

$$SL(i) = \sum j \in controllers(i)((1 - pcj \times slj) \times \sum j \in controllers(i) tlk) \quad (3)$$

where, function controllerst(i) returns all trusting controllers of a segment i.

we can first calculate the privacy risk (PR(i)) and the sharing loss (SL(i)) for each conflict segment (i), individually. Finally, following equation can be utilized to make the decisions (permitting or denying conflicting segments) for privacy conflict resolution, guaranteeing to always find an optimal solution.

$$Decision = \begin{matrix} Permit\ if\ \alpha SL(i) = \beta PR(i) \\ Deny\ if\ \alpha SL(i) < \beta PR(i) \end{matrix} \quad (4)$$

Where α and β re preference weights given to privacy risk and sharing loss.

After finding the values of privacy risk and sharing loss, a decision is made on the list of accessors in the conflicting segments who can have the access to the data. Finally, the permitted users in the conflicting segment and all the accessors in the non conflicting segments are given access to the shared data item.

CONCLUSIONS

In this paper we have proposed a multiparty access control model for the collaborative management of shared data. In this approach each of the controllers of the data item has the right to set the privacy policy settings on the data item such that the controllers can specify who can see or cannot see the shared data item. Also we have implemented a solution for privacy conflict detection and resolution for collaborative data sharing in OSNs. Our conflict resolution mechanism considers privacy-sharing tradeoff by quantifying privacy risk and sharing loss.

FUTURE ENHANCEMENT

The proposed system is restricted to deal with photo sharing in online social networks. The future work of this model can be extended to deal with different kinds of files such as audio files, video files, documents and even comments in a post or an image. Also, we would extend our work to address security and privacy challenges for emerging information sharing services such as location sharing and other social network platforms.

REFERENCES

1. Facebook Privacy Policy. http://www.facebook.com/policy.php/.
2. Facebook Statistics. http://http://www.facebook.com/press/info.php?statistics.
3. Hongxin Hu, *Member, Gail-Joon Ahn, and Jan Jorgensen*, "Multiparty Access Control for Online Social Networks: Model and Mechanisms", IEEE Transactions On Knowledge And Data Engineering, July 2013
4. G. Ahn and H. Hu. Towards realizing a formal rbac model in real systems. In Proceedings of the 12th ACM symposium on Access control models and technologies, pages 215–224. ACM, 2007.
5. P. Fong. Preventing sybil attacks by privilege attenuation: A design principle for social network systems. In Security and Privacy (SP), 2011 IEEE Symposium on, pages 263–278. IEEE, 2011.
6. B. Carminati, E. Ferrari, and A. Perego. Rule-based access controlfor social networks. In *On the Move to meaningful Internet Systems2006: OTM 2006 Workshops, pages 1734– 1744. Springer, 2006.*