IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VI (Sep-Oct. 2014), PP 55-61
www.iosrjournals.org

Collaborative data sharing in online social network resolving privacy risk and sharing loss

Nithya Sara Joseph
(M.Tech Computer Science, Caarmel Engineering College, MG University, India)

Abstract : *Nowadays, Online Social Networks (OSNs) is popular all over the world. Millions of people join such networks to share their personal and public information and also to make new friends and relations. But there arises several security and privacy issues related to these network since users may have contact with persons who are known to them as well as unknown to them. There are many mechanisms to provide privacy on shared data but enforcing privacy concerns over data associated with multiple users is of great concern as there are chances for privacy risk and data sharing loss. In this paper, privacy setting for a shared data is discussed where multiple users, other than owner, who shares the same data can provide their own privacy policies on shared data.. Privacy conflicts are resolved using a conflict resolution mechanism which will calculate the privacy risk and sharing loss associated with each controller. Thus in this paper a systematic solution that facilitate collaborative management of shared data in OSNs and a conflict detection and resolution mechanism to cope with privacy conflicts in data sharing is addressed.*

Keywords: *Access control, Data sharing, Privacy conflict, Social network*

I. Introduction

Online Social Network is a web-based service that allows each individual to construct a public or semi-public profile within the service; shows a list of users with whom they can share information; view and traverse their list of information and also those made by others within the service. There are plenty of social networking sites in Internet each having different types of people who have a something in common to discuss with, for example Facebook, google+, twitter, LinkedIn, etc. Millions of people have joined such networks, Facebook, one of the social network sites, claims that it has about 1.11 billion monthly active users, globally. People are allowed to upload multimedia contents and share many aspects of their personal life. Due to the public nature of OSN, especially Internet itself, the content of the user may be disclosed to a wider audience than they actually intended for. Most users who publish contents in the social network are unaware of its features. Since OSNs store a high amount of sensitive as well as private information of users. Protecting such information is of great concern. Therefore access control mechanisms are essential for protecting user data in OSNs [2].

Each user is provided with a virtual space to keep their information in the OSN. Furthermore, user is allowed to upload content to his space and also to other's spaces also. He can also tag other users, which is an explicit reference that links to a user's space. Current OSN provide privacy control mechanism which allow users to regulate access to the data contained in their own spaces only, they do not have any control for data residing outside the spaces. For e.g. if a person A post a comment on other user B's space, the contributor of the content cannot specify any privacy policy. Only the owner has got the right of setting privacy. Similarly, if a person uploads a photo on to his space and tags his friends in that, tagged persons in the photo cannot set any privacy. OSNs also enable users to share others' content. For example, when person A views a photo in person B's space and decides to share this photo with his friends, the photo can be posted to his space and he can authorize his friends to see this photo. Here, A may adopt a weaker access control saying the photo is visible to everyone, the initial privacy concerns related to owner of this photo may be violated, resulting in the leakage of sensitive information while publicizing data [12]. The privacy conflicts may also occur in two other situations, profile sharing and friendship sharing. This is because data shared by multiple associated users may have different privacy concerns and the lack of collaborative privacy control increases the potential risk in leaking sensitive information by friends to the public. The following fig.1 shows a scenario where a privacy conflict can occur on sharing data between multiple users in a social network. It explains privacy conflict scenario in content sharing where sharing starts from a contributor who uploads content, and then a disseminator views and share the content.

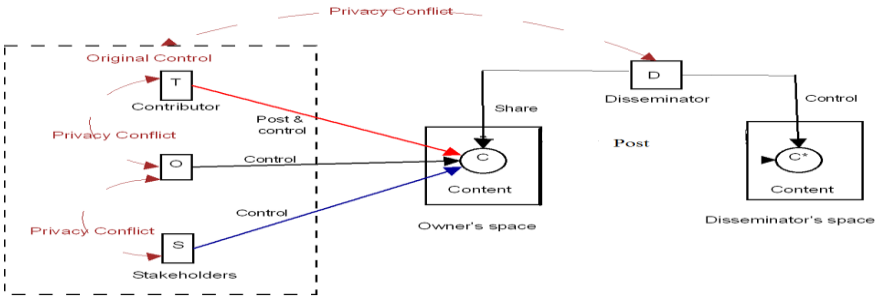


Fig. 1 Privacy conflicts in OSNs

In this paper, an effective mechanism to provide control for multiple users on the shared data as well as an algorithm to thwart privacy risks and data sharing loss is been discussed. Also a proof-of-concept prototype of my approach is implemented based on social network developed by myself.

II. Related Work

Security and privacy in social network is now becoming an important research area nowadays. When a user uploads information in OSN they have a scope in mind and the privacy involves keeping that information's within the intended scope. Scope can be defined as size of the audience, extent of usage allowed, and duration of the content. Privacy is breached when information is moved beyond this scope. Case studies show that most users do not change their default privacy settings provided by the OSNs there by creating privacy issues. Current OSNS demands user to be system and policy administers for regulating their data, where users can restrict data sharing to a specific set of trusted users.

In literature [6, 7, 8, 9], several proposals of an access control scheme for OSNs have been introduced. But most of them were based on the property of trust. For example, Carminati et al. [6] introduced a trust-based access control mechanism, which allows the specification of access rules for online resources where authorized users are denoted in terms of the relationship type, depth, and trust level between users in OSNs. They also proposed a semi-decentralized discretionary access control system and an enforcement mechanism for controlled sharing of information in OSNs. Fong et al. [8] proposed an access control model that deals with the access control mechanism implemented in Facebook. Gates [13] described a new method where access control was based on relationship which is a new security paradigm that addresses the requirements of the Web 2.0. Then, Fong [9] recently formulated a paradigm called a Relationship-Based Access Control (ReBAC) where, the authorization decisions was based on the relationships between the resource owner and the resource accessor in an OSN. However, these works couldn't accommodate privacy control requirements with respect to the data sharing in OSNs. Several recent works in access control mechanism recognized the need of joint management for data sharing, in OSNs, especially in the area of photo sharing. Squicciarini et al. [11] proposed a solution for privacy management for photo sharing in OSNs. In this work they considered the privacy control of a content that is co-owned by multiple users in an OSN, where each co-owner may separately specify his/her own privacy preference for the shared content. The Clarke-Tax mechanism was adopted to provide the collective enforcement in the shared content. Evaluation of the scheme was done by applying Game theory. However, the drawback of this solution is the usability issue and they do not accommodate all stakeholders' privacy preferences. Hongxin Hu et.al, [12] proposes a simple but flexible mechanism for collaborative management of shared data in OSNs associated with multiple users. Even though they addressed multiparty access control issues, chances of privacy risk and data sharing loss are high due to a simple conflict resolution strategy. In contrast, in this work an effective conflict resolution solution is introduced, which makes a trade off between privacy protection and data sharing by considering the privacy concerns from multiple associated users.

III. Proposed Work

OSNs like Facebook supports only single user privacy but for a multiuser environment this privacy mechanism is not appreciable. Therefore, a collaborative management of shared data with respect to multiple controllers in OSNs as well as more suitable method for identification and resolution of privacy conflict is been discussed here. At first, a model for collaborative sharing is defined and then a privacy policy scheme is introduced for the specification and enforcement of multiparty privacy concerns. Then, systematic method is articulated for identifying and resolving privacy conflicts derived from multiple privacy concerns for collaborative data sharing in OSNs.

3.1 Model for Collaborative Control in Data Sharing in OSNs

3.1.1 OSN Representation

OSN is a network of users who share same ideas, thoughts, interests, and so on. Usually a network is represented using a graph, where each node of the graph denotes the user and the edges represent the relationship between two users. Following section describes an abstract representation of an OSN with the core components upon which to build our solution:

• U is a set of users in the OSN, where each user has given a unique identifier;

• G is a set of groups to which the users in an OSN can belong,

•$UU \subseteq U \times U$ is a binary user-to-user friendship relation in an OSN;

• $UG \subseteq U \times G$ is a binary user-to-group membership relation in an OSN;

• P is a collection of user profile sets, $\{p_1, \ldots, p_o\}$, where p_i is the profile of a user $i \in U$. Each profile entry can be a tuple consisting of <attribute: profile-value> pair;

• F is a collection of user friend sets, $\{f_1, \ldots, f_q\}$, where f_i is the friend list of a user $i \in U$ in OSN;

• C is a collection of user content sets, $\{c_1, \ldots, c_s\}$, where ci is a set of content of a user $i \in U$; and

• D is a collection of data sets, $\{d_1, \ldots, d_u\}$, where $d_i = p_i \cup f_i \cup c_i$ is a set of data of a user $i \in U$.

• *CT* = {*OW, CO, ST, DS}* is a set of controller types, indicating *ownerOf*, *contributorOf*, *stakeholderOf*, and *disseminatorOf*, respectively;

3.1.2 Privacy Policy Specification for Collaborative Sharing

To ensure collaborative sharing among users in an OSN some policies should be specified. The main elements for a collaborative sharing are controllers, accessors, and the shared data itself. For each element we specify some rules to identify them.

Controller Specification: In addition to the owner of data, other controllers such as the contributor, stakeholder and disseminator of data, also need to regulate the access of the shared data in OSNs. Each can be defined as follows:

Owner: Let d be a data item in the space of a user U in the social network, then user U is called the owner of d, denoted as OW .

Contributor: Let d be a data item published by a user U in the space of another user U' in the social network, then user U is called the contributor of d, denoted as CO .

Stakeholder: Let d be a data item contained in the space of a user U' in the social network. Let G be the set of tagged users associated with d. A user U is called a stakeholder of d, denoted as ST, if $U \in G$.

Disseminator: Let d be a data item shared by a user U from the space of another user U' to his/her space in the social network. The user U is called a disseminator of d, denoted as DS.

Then the controller specification can be defined as follows:

Controller Specification: Let $cn \in U$ be a user who can regulate the access of data in multiuser environment. And let $ct \in CT$ be the type of the cn, then the controller specification is defined as a tuple < cn,ct >.

Accessor Specification: Accessors are a set of users to whom the authorization is to be granted. Accessors can be represented with a tuple consisting of user names, the friendship or a set of group names in OSNs. To facilitate collaborative privacy management, trust levels can be included, which are assigned to accessors when defining the privacy policies. The notion of accessor specification can be formally defined as follows:

Accessor Specification: Let a be a user $u \in U$, accessor can be denoted by; $a \in U \cup \{friendOf\} \cup G$. Let tl be a trust level, which is a rational number in the range of[0,1], assigned to a. And let $at \in \{UN, FS, GN\}$ be the type of the accessor (user name, friendship, and group name, respectively).The accessor specification is defined as a set, where each element is a 3-tuple <a, tl, at >.

Data Specification: In the context of OSNs, user data is composed of three types of information; user profile, user friendship, user content. To facilitate effective resolution of privacy conflicts for collaborative privacy control, sensitivity levels are introduced for data specification, which are assigned by the controllers to the shared data. The users' judgment of the sensitivity levels of the data is multi-dimensional with varying degrees of sensitivity. The data specification can be formally defined as follows:

Data Specification: Let $da \in D$ be a data item, and sl be a sensitivity level, which is a rational number in the range [0,1], assigned to da. The data specification is defined as a tuple < da,sl >.

Privacy Policy: To summarize the above features and elements, a formal definition of privacy policies for collaborative data sharing can be defined as follows:

Privacy Policy: A privacy policy is a 4-tuple P = <controller, accessor, data, effect >, where controller, accessor, and data are defined above in the definitions. The element effect in tuple, can be defined as: effect ∈ {permit, deny} is the authorization effect of the policy.

3.1.3 Policy Evaluation

There are mainly two steps to be performed to evaluate an access request over MPAC policies. In the first step, it checks the access request against the policy specified by each controller and yields a decision for each controller. The *accessor* element in a policy specified decides whether the policy is applicable to a request. If the user who sends the request for the access belongs to the user set derived from the *accessor* of a policy, the policy is applicable to the user and the evaluation process returns a response with the decision permit indicated by the *effect* element in the policy. Otherwise, the response yields deny decision. In the second step, decisions from all controllers are aggregated to make a final decision for the access request. Fig.2 shows evaluation process in detail.

Once policy evaluation is done we will get a set of accessors for whom access can be guaranteed. Conflicts may occur as different controllers may have different decisions. To resolve those conflicts during multiparty policy evaluation, it is essential to adopt a systematic conflict resolution mechanism to adopt an unambiguous decision.

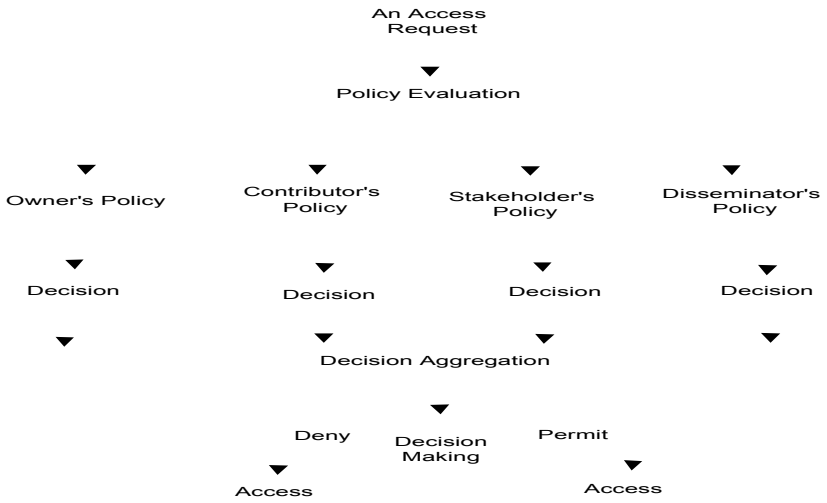


Fig.2 Multiparty policy Evaluation process

3.2 Identification and Resolution of Privacy Conflict in Collaborative Data Sharing

A *simple* solution for resolving multiparty privacy conflict is to allow common users of the multiple controllers to access the data item. But this method is too restrictive in many cases and can produce undesirable results for resolving multiparty privacy conflicts.

Another method is to use a *strong* conflict resolution method, which may provide a better privacy protection. But problem is that, it may reduce the social value of data sharing in OSNs. To address these issues, a new mechanism for resolving multiparty privacy conflicts in OSNs is discussed.

3.2.1 Privacy Conflict Identification

Each controller of the shared data specifies a set of trusted users who can access the data. The set of trusted users represent the accessor space of the controller. First, we have to partition the accessor space of all controllers into disjoint segments and then we have to identify the conflicting accessor space segments in them. Each conflicting segment contains at least one privacy conflict in them. To illustrate this, consider the venn diagram shown in Fig. 3. Suppose we have 3 controllers, say, C1, C2 and C3 for a shared data item. The accessor space for each is represented by a circle in the diagram. Overlapping spaces shows the accessor space defined by multiple controllers. When space segmentation is done we will get seven disjoint segments as shown below. The space segments can be classified into two categories: non-conflicting segments and conflicting segments. Non-conflicting segments are those that represent accessors who are trusted by all controllers, denoted by segment ps. Conflicting segments are those that represent accessors who are not trusted by all controllers. In the figure segments CAS4, CAS5 and CAS6 represents conflicting accessor space with two privacy conflicts while segments CAS1, CAS2 and CAS3 represents conflicting accessor space with privacy conflict one, respectively.

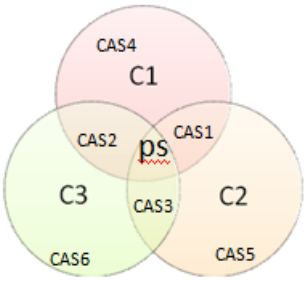


Fig 3. Example of Accessor space segment and privacy conflict identification.

Accessor spaces of the controllers are segmented using the pseudo code shown in algorithm 1. A function called Divide() accomplishes this procedure. This function will add an accessor space fl_a, derived from policies of an controller a, to an accessor space set S. A pair of accessor spaces must satisfy one of the following relations: subset, superset, partial match, or disjoint. Therefore, the overlapped spaces are separated into disjoint spaces using set operations. A set of conflicting segments has the following properties:

1) All conflicting segments are pairwise disjoint: $cas_i \cap cas_j = \emptyset$, $1 \leq i \neq j \leq n$;

2) Any two different accessors a and a′ within the same conflicting segment (cas_i) are defined by the exact same set of controllers: GetController(a) = GetController(a′), where $a \in cas_i$, $a' \in cas_i$, $a \neq a'$;and

3) The accessors in any conflicting segments are untrusted by at least one controller of the shared data item.

Algorithm 1.Identification of conflicting segments

Input: A set of accessor space, AS.
Output: A set of disjoint accessor space, CAS.

```
1   S:= Divide(AS); /* Partition  the entire accessor space*/
2   CAS.New(); /*Identify the conflicting segments*/
3   foreach s∈S do
4           C:=GetControllers(s);/*Get all controllers associated with segment s*/
5           if |C| < |AS| then
6           CAS.Append(s); /*append the conflicting segment to CAS*/
7            Divide(AS)
8           foreach a∈AS do
9                   fl_a:= FriendList(a);
10                  foreach s∈ S do
11                          if fl_a ⊂ s then
12                           S.Append(s \ fl_a);
13                           S:= fl_a ;
14                           Break;
15                           else if fl_a  ⊃ s then
16                                   fl_a := fl_a \s;
17                                   else if fl_a ∩ s ≠ ∅ then
18                                           S.Append(s \ fl_a);
19                                           s := fl_a∩ s;
20                                           fl_a:= fl_a \ s;
21  S.Append(fl_a);
22  return S;
```

3.2.2 Privacy Conflict Resolution

A decision to allow or deny access for a shared data by a set of accessors in a conflicting segment is determined by the process of resolution method. There are two problems that can occur at this time, i.e., privacy risk and data sharing loss.

Measuring Privacy Risk: Privacy risk of a controller helps to identify the potential threats that can occur in that segment. Privacy risk of a controller can be measured using following parameters:

• Number of privacy conflicts: It is the number of untrusting controllers in a conflicting segment. The untrusting controllers of a conflict segment i are returned by a function $controllers_{ut}(i)$;

• General privacy concern of an untrusting controller: Different controllers may have different general privacy concern for the same kinds of data. For example, public figures may have higher privacy concern on their shared photos than ordinary people. General privacy concern can be derived from default privacy settings of the controller, denoted by $pc_{j;}$
• Sensitivity of the data item: It is perception of the controller about the confidentiality of the data shared by the. The factor is depended on each controller, denoted by sd_j for each untrusted controller j;
• Visibility of the data item: It defines how many accessors contained in a segment can view the shared content. The more the accessors in a segment, the higher the visibility; and
• Trust of an accessor: The trust level of an accessor k is the average value of the trust levels defined for it by the trusting controllers of the conflicting segment, denoted by tl_k.

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

$$\mathrm{PR(i,j)} = \sum_{j \in controllersut(i)} \left(PR(i,j)\right)$$

$$\mathrm{PR(i,j)} = \sum_{j \in controllersu_t(i)} pc_j \times sd_j \times \sum_{k \in accesors(i)} (1 - tl_k) \quad (1)$$

Measuring Sharing Loss: A sharing loss is said to occur when the decision of privacy conflict resolution is to deny access on certain shared data but some controllers expect their accessors to access the same. All the four factors used for measuring privacy risk is used and instead of number of privacy conflict here number of trusting controllers is used. The overall sharing loss SL(i) of a conflicting segment i can be computed as follows:

$$\mathrm{SL(i)} = \sum_{j \in controllers_t(i)} ((1 - pc_j \times sd_j) \times \sum_{k \in accesors(i)} tl_k) \quad (2)$$

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

For an effective privacy conflict resolution a mechanism is needed to balance the privacy protection and data sharing. Finally the following equation is used to make decisions for guaranteeing the access for conflicting segments.

$$\text{Decision} = \begin{cases} \text{Permit} & \text{if } \alpha \mathrm{SL(i)} \geq \beta \mathrm{PR(i)} \\ Deny & if\ \alpha \mathrm{SL(i)} < \beta PR(i) \end{cases} \quad (3)$$

α *and* β are the weight assigned for privacy risk and sharing loss such that $\alpha + \beta = 1$, $0 \leq \alpha,\beta \leq 1$.

When privacy conflicts are resolved a new accessor list (AL) can be generated with permitted conflicting segments and non-conflicting segments.

IV. Implementation And Evaluation

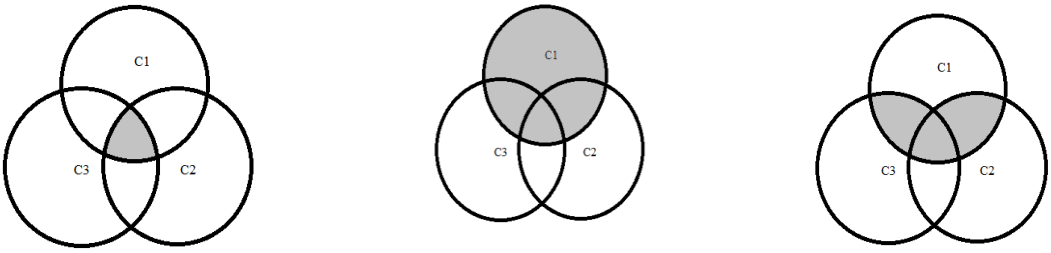
4.1 Prototype Implementation

As a proof for the concept a demo social network called Friends is implemented. Like Facebook, Friends also allow its users to create their own profile; post comments, upload photos and videos also view other users profile and their data. But unlike Facebook, where only the owner of the data has the control to set privacy, here all the controllers of a shared data can set privacy for themselves. Each user of the application has to mention their privacy concern for that network at the time registration. When a user login to his account, he is able to see all the data that he has access to. At the time of login the application searches the database to see for what all data the user is a controller or an accessor. If he is a controller of some data, he can set privacy for that shared data. For that an access link is provided near to the content. When the controller click the access link, he is given the option to set the users or groups with whom he wish to share the data as well as trust level of each user and the sensitivity of the shared data to calculate privacy risk and sharing loss. If he is an accessor to some data, the application performs policy evaluation, i.e, decision of all controllers are taken and aggregated and also privacy conflicts, if any, are identified and resolved to make final decision whether to permit or to deny access to the shared data.

4.2 Evaluation

The evaluation of my approach is done by comparing with the naive solution, and also with the privacy control solution used by existing OSNs, such as Facebook with respect to two metrics, privacy risk and sharing loss. To explain this, consider the example in Fig.4, where three controllers desire to regulate access of a shared data item. The naive solution allows only the accessor in the non-conflicting segment to access the data item as shown in Fig. 4(a). Thus, the privacy risk is 0 for this solution. However, the sharing loss is the absolute

maximum, as all conflicting segments, which may be allowed by at least one controller, are always denied. The Facebook allows the owner the highest priority and therefore owner's decision will be final. Therefore, all accessors within the segment covered by the owner's space are allowed to access the data item, but all other accessors are denied as illustrated in Fig. 4(b). Here, the owner's privacy risk and sharing loss are both 0. However, the privacy risk and the sharing loss are large for every other controller. According to my solution, each conflicting segment is evaluated individually. Then CAS1 and CAS2 become permitted conflicting segments along with ps after resolving the privacy conflicts. Fig. 4(c) demonstrates the result of our privacy conflict resolution. Thus privacy risk and data sharing loss is minimized in Prototype.



(a) Naive solution (b) Facebook (c) Prototype

Fig. 4 Example of Resolving Privacy Conflicts.

V. Conclusion

Online social networks help people to socialize with the world. But users should be aware of threats that can be faced due to lack of proper privacy settings. In this paper a novel method for collaborative sharing of data in OSNs is discussed as well as a method to resolve privacy conflicts that can occur while multiple persons share a data. Evaluation results show that privacy risk and data sharing loss are minimized in this approach. As a part of future work, I would like to study on complex security policies to ensure more protection against collusion attacks. Since setting privacy is a time consuming process, would like to investigate a good machine learning algorithm to minimize the same.

References

[1] Facebook Developers.http://developers.facebook.com/.
[2] Facebook Privacy Policy, htttp://www.facebook.com/policy.php/.
[3] 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.
[4] G. Ahn,H. Hu, J. Lee, and Y.Meng. Representing and reasoning about web access control policies. In Computer Software and Applications Conference(COMPSAC),2010.IEEE 34th Annual, pages 137–146. IEEE , 2010.
[5] B. Carminati and E. Ferrari. Collaborative access control in online social networks. In Proceeding of the 7thInternational Conference on Collaborative Computing: Networking, Applicationsand Worksharing pages 231–240. IEEE, 2011.
[6] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In On the Move to Meaningful Internet Systems2006: OTM 2006 Workshops, pages 1734–1744. Springer, 2006.
[7] B. Carminati, E. Ferrari, and A. Perego. Enforcing access control in web-based social networks. ACM Transactions on Information and System Security (TISSEC), 13(1):1–38, 2009.
[8] 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.
[9] P.Fong, M.Anwar, and Z.Zhao. A privacy preservation model for facebook - style social network systems. In Proceedings of the 14th European conference on Research in computer security, pages 303–320. Springer-Verlag,2009.
[10] H.Hu, G.-J. Ahn, and J. Jorgensen. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In Proceedings of the 27th Annual Computer Security ApplicationsConference, ACSAC '11, pages 103–112. ACM, 2011.
[11] A. Squicciarini, M. Shehab, and F. Paci. Collective privacy management in social networks. In Proceedings of the 18th international conference on World wide web, pages 521–530. ACM, 2009.
[12] H.Hu, G.-J. Ahn, and J. Jorgensen. Multiparty Access Control for Online Social Networks: Model and Mechanisms, IEEE Transactions On Knowledge And Data Engineering,2013.
[13] 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.