An Access Control Model for Shared Data in Online Social Networks

Sreeprabha S[1], Final Year M.Tech and Jisha Jose[2], Asst.Professor
Department of Computer Science and Engineering
Mar Baselios College of Engineering And Technology
Trivandrum

Abstract— In recent years, we have seen unprecedented growth in most of the popular Online Social Networks (OSNs) and become a concerning fact for web access with billions of variant regular internet users worldwide. These OSNs propose good-looking means for virtual social connections and social as well as personal information sharing between users. At the same time they additionally move up a no. of security and privacy issues. Of course present OSNs permit a single user to limit access to his/her shared data. But they do not offer any method to implement privacy concerns over data connected with multiple users leading to potential disclosure of information. To overcome this, an efficient approach is proposed to facilitate the protection of collaborative privacy management of shared data connected with multiple users in OSNs. In this paper a systematic mechanism is provided to identify and resolve privacy conflicts for collaborative information sharing. This paper presents Multi Party Access Control (MPAC) model to take into custody the core features of multiparty authorization framework which includes multiparty policy specification scheme and policy evaluation mechanism to protect sensitive data from undesired accesses.

Index Terms—Data Sharing, Decision Voting, Mcontroller, Multi Party Access Control, Multiuser, Online Social Network, Policy Specification, Privacy

I. INTRODUCTION

Online Social Networks (OSNs) like Facebook, Google+, Twitter, etc. plays a vital role in the daily life of many users. It is used to find and communicate with known persons such as friends, colleagues, family members and even with unknown ones. The communication is based on user request and response. When the user accepts the request of another they can share information such as photos, messages, videos, etc.

Manuscript received December, 2014.
Sreeprabha S[1], Final Year M.Tech, Department of Computer Science and Engineering, Mar Baselios College of Engineering And Technology Trivandrum.

Jisha Jose[2], Asst.Professor, Department of Computer Science and Engineering, Mar Baselios College of Engineering And Technology Trivandrum.

OSN is a feature essentially designed to facilitate people create profile, manage their profiles, make social interactions and to share tremendous amount of data with other users for various needs. Users profile usually includes information such as user's name, birth date, contact information, email, interests, photos, music, videos and many other attributes.

In OSNs, the users can post messages, upload videos and photos in their own spaces, tag other users to their data, share data with their friends, and also post content in their friends profile. Each tag is an explicit reference that links to a user's profile. The shared data is associated with multiple users. Suppose a photo contains three users, Dave, Eve and Frank. Assume Dave uploads it to his own space and tags both Eve and Frank. Here Dave is the owner and Eve and Frank are stakeholders of the photo. Each of them can specify privacy policies to control over that whom can see that photo. Since each associated user may have different privacy concerns over that shared data, privacy conflicts can occur among them and lack of collaborative privacy control increases the privacy risk in leaking sensitive data by friends to the public.

Only limited security is maintained in the process of information sharing in social networks. While sharing the information like photo to another one there is a chance to share information by third person. The potential privacy risks of such cases are ignored. For example, users often publish personal information to a wider audience than expected. They also post data about others without their permission. However there is a mismatch between users' needs for personal data sharing and what online social networks today offer. In order to overcome this issue a policy is generated for the information to be shared with the other. If anyone who satisfies this policy they are permitted to watch those photos, videos, etc. otherwise not eligible.

A lack of experience and awareness in users as well as proper tools and design of OSNs turn the situation worse. The tools for sharing information in OSNs can cause various privacy issues. This paper aims to provide insight into such privacy issues in OSNs, their associated privacy risks and existing research into solutions. The main security mechanism used to handle such issues is the access control. The unexpected growth of sensitive information that is easily available in social networks has elevated an expectation for effective access control that can protect that information from untrusted users. Another problem in

ISSN: 2278 – 7798

online social network is conflict among access rules defined by each user. Privacy policies conflict each other when a user denies everyone from accessing his own data but his friends allow others to see it. The proposed model is used to resolve this conflict by different priority levels for the rules. The logical foundation of the model gives flexibility and accuracy and finally the risk of sharing data in online social networks is decreased. This paper gives a method dealing with major security concerns and thus providing a multiparty access control over shared data connected with multi users.

II. LITERATURE REVIEW AND 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 provides the specification access rules for online resource where authorized users are denoted in terms of the relationship type depth and trust level between users in online social networks. Semi-decentralized discretionary access control model and a related enforcement mechanism for controlled sharing of information in OSNs. 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 [6]. The sharing of data especially photo sharing in online social network Squicciarini et al provided a solution for collective privacy management in online social networks [7]. 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 [8]. In contrast, this work proposes a formal model to address the multiparty access control problem 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, this solution can also conduct various analysis tasks on access control mechanisms used (Hu et al, 2011) (Hu et al , 2012).

III. PROBLEM STATEMENT

Current OSNs provide a simple access control mechanism that allows users to control access to information contained in their own spaces. Unfortunately, users have no control over data residing outside their spaces. Assume that, if a user posts a data in a friend's space, he/she cannot mention which users can view the comment. Similarly, when a user uploads a photo and tags friends who appear in the photo. Even though the tagged friends may have different privacy concerns about the photo the user cannot regulate who can see this photo. To address such a critical issue, existing OSNs provide only preliminary protection mechanisms [5]. For example, Facebook allows tagged users to remove the tags linked to their profiles or report violations asking Facebook managers to remove the contents that they do not want to share with the public. But several limitations are suffered by this simple protection mechanism. Also, removing a tag from a photo can only prevent other members from seeing a user's profile since each tag is an explicit reference to user's space, but the user's image is still contained in the photo. The user's image continues to be disclosed to all authorized users since original access control policies cannot be changed. Moreover, reporting to OSNs only allows users to either keep or delete the data. Such a binary decision is either too restrictive. So it is necessary to develop an effective and flexible access control mechanism for OSNs, accommodating the authorization requirements coming from multiple associated users for managing the shared data collaboratively [2].

IV. MULTIPARTY ACCESS CONTROL FOR OSNS

Current OSNs provide the data owner to govern the shared data item. But it does not provide a mechanism to specify and enforce the privacy concerns from associated users. This will lead to privacy conflicts which is unresolved and sensitive information being potentially disclosed to the public [2]. This section provides a collaborative privacy management approach for the protection of shared data associated with multiple users in OSNs. A privacy policy mechanism is first developed for the specification and enforcement of multiparty privacy concerns. Then, a systematic method is generated for identifying and resolving privacy conflicts derived from multiple privacy concerns for collaborative data sharing in OSNs.

A. MPAC Model

An Online Social Network, such as Facebook, typically consists of group of users, group of user profiles, user contents, and a group of user relationships. Existing OSNs do not provide effective mechanism to support privacy control over shared data. The core components for representing an OSN to build the MPAC model are [1]:

- $U= \{u_1, u_2....u_n\}$ is a group of users of the OSN. A unique identifier is provided for each user.

ISSN: 2278 – 7798

- G= {$g_1, g_2....g_m$} is the set of groups to which user can belong. A unique identifier is provided for each user.
- $UU \subseteq U \times U$ is a binary user-to-user friendship relation;
- $UG \subseteq U \times G$ is a binary user-to-group membership relation;
- $P= \{p_1. . . p_o\}$ is a set of user profile sets, , where $p_i = \{p_{i1}, . . . , p_{ip}\}$ is the profile of a user $i \in U$. Each entry in user profile is a <*attribute: profile-value*> pair, $p_{ij} =< attr_j : pvalue_j >$, where $attr_j$ is an attribute identifier and $pvalue_j$ is the attribute value;
- $F=\{f_1,f_2...f_q\}$ is a set of user friend sets, where $f_i = \{u_1, . . . , u_r\}$ is the friend list of a user $i \in U$;
- $C=\{c_1,c_2...c_s\}$ is a set of user content sets, where $c_i = \{c_{i1}, . . . , c_{it}\}$ is a set of content of a user $i \in U$, where cij is a content identifier; and
- $D= \{d_1, d_2 \ldots d_u\}$ is a group of data sets, where $d_i = p_i \cup f_i \cup c_i$ is a set of data of a user $i \in U$.

B. MPAC Privacy Policy Specifications

Privacy policies are necessary to regulate access over shared data to enable collaborative management of sharing data items in OSNs. Several access control schemes [9, 5] can allow only a single user to specify his/her privacy concern. A flexible privacy control method in social networks should allow multiple controllers associated with a single data.

Controller Specification

Owner Module:

In the Online Social Network, owner module is defined as the owner of the shared data item dϵ D is the user uϵ U, if d is published in the space m of user u by himself. The user is also known as contributor of d, if data item d is shared by user. It is denoted by OR_d^u.

Contributor:

In the contributor module of online social network, let the user uϵ U publish a shared data item dϵ D in another user's space, then the user u is called contributor of d. It is denoted by CR_d^u.The content tagged by contributor to someone else's space have multiple tagged users.

Stakeholder:

In the stakeholder module of online social network, if the user uϵ U is called stakeholder of shared data item dϵ D published in the space of another user in the same online social network. It is denoted by SR_d^u. Let S be the set of tagged users connected with d, then uϵ S.

Disseminator:

In the disseminator module of online social network, the user uϵ U shared a data item dϵ D from another user's space to his/her own space. Then that user u is called disseminator of data d. It is denoted byDR_d^u. The disseminated content can be again disseminated.

Definition: Let cn ϵ U be a user who can regulate the access of shared data item. Also let ct ϵ CT be the type of the cn, where CT= {OR, CR, SR, DR} is a set of controller types, representing Owner, Contributor, Stakeholder and Disseminator. The controller specification is formally defined as a 2-tuple <cn,ct>[2].

Accessor Specification

The set of users whom the gain to access the user's shared content is permitted is called accessors. In online social networks, they are specified with a set of users with their names, group names or relationship. Here the relationship factor is restricted to friendship (i.e., friendOf relation). We literarily defined the idea of Accessor Specification as follows:

Definition: The Accessor Specification is defined as a set of accessors A= {$a_1, a_2 \ldots a_n$} where each element is a 2-tuple <u,t> where u be a specific user uϵ U, a group gϵ G or the relation friendship that is uϵ U$\cup${friendOf}$\cup$G. And let t ϵ {UN, GN, FS} be the type of the accessor where (User Name, Group Name, and Friendship respectively) [1].

Data Specification

In the online social networks, the user data is a collection of data sets where each element is represented as user profile which describes details of each user such as name, birth date, contact information, identity etc, relationship of user like list of friends, family members etc and content in user's profile like photos, videos etc.

Again to open the door for successful resolution of privacy conflict different controllers launch sensitivity level on shared data item for collaborative multiparty access control in Data Specification. Here the users' judgment of the sensitivity levels of shared data item is multi-dimensional. The concept of Data Specification is formally defined as:

Definition: Let D= {$d_1, d_2 \ldots d_n$} where $d_i \epsilon$ C$\cup$P$\cup$G be the data item and sensitivity level ranging from 0.00 to 1.00. The Data Specification is defined as 2 tuple <di,sl> [4].

MPAC Policy

A multiparty access control (MPAC) privacy policy is the combination of controller specification, accessor specification and data specification. For collaborative management of data sharing it is formally defined as follows:

A MPAC policy is a 4-tuple MP = < controller, accessor, data, effect>, where

- controller is defined in controller specification
- accessor is defined in accessor specification
- data is defined in data specification
- effect ϵ {permit, deny} which is the final effect of MPAC policy.

Assume that a controller can allocate five sensitivity levels to a user indicating *none* (0.00), *low* (0.25), *medium* (0.50), *high* (0.75) and *highest* (1.00) for the shared data item . Similarly a controller can allocate five trust levels to a user indicating *none* trust (0.00), *low* trust (0.25), *medium*

ISSN: 2278 – 7798

trust (0.50), *high* trust (0.75) and *highest* trust (1.00) . Some examples for access control policy.

Example 1: Bob authorizes his friends to access a photo *mypic.jpg* with medium sensitivity level, where Bob is the owner of photo.

P1= (Bob, OR,{<friendOf, FS>},<mypic.jpg,0.50>, permit)

C. MPAC Evaluation

The evaluation process of multiparty access control policies consists of three steps. The initial step deals with checking the policy specified by controller against the access request. In the second step, individual decisions from each controller corresponding to the access request are taken. Fig.1 illustrates the multiparty access policy evaluation process.

For an access request, multiple controllers have different privacy concerns over the shared data item. Also they may have different decisions either as permit or deny. The evaluation process then checks whether any conflict exists between individual decisions. To resolve such conflicts it is necessary to choose an efficient conflict resolution procedure at the time of policy evaluation to produce an unambiguous final decision.

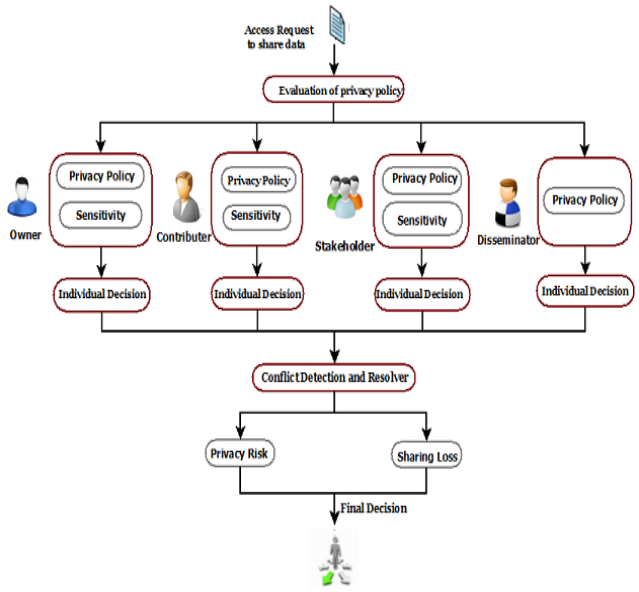

Fig.1: MPAC Architecture

Privacy Conflict

A privacy conflict occurs when two or more users disagree to expose a shared data item. The key factor leading to privacy conflicts is the contradictory privacy concerns over the shared data item which is associated with multiple users. Consider an example with two controllers of a photo. Let them be Carol and Eve. Each controller specifies their own privacy policy such that only his/her friends can see the photo. It is not possible that these two controllers have similar set of friends. Thus there exists the privacy conflict in case of shared data item.

For resolving multiparty privacy conflicts the only simple solution is to permit the recurrent users to access the data specified by the multiple associated controllers of the shared data item. But this solution is not beneficial and hence not produces better results. Assume that there are four users/controllers, Carol, Eve, Frank and Oscar, and each of them permits their own friends to view a particular photo. Let Carol, Eve and Frank have many common friends with each other. The fourth user named Oscar has a poor privacy concern on that photo. At last in this case no one can access the photo. To furnish a strong privacy protection, a strong conflict resolution approach is needed. The first step to find a consistent solution for resolving these multiparty privacy conflicts is to launch a method for identifying privacy conflicts [2].

Identifying Privacy Conflicts

A group of trusted users who can access the shared data item is defined by each controller. The controllers' accessor space consists of group of trusted users. The accessor spaces of all controllers of a shared data item are partitioned into disjoint segments using space segmentation procedure [12]. The conflicting accessor space segments consist of controllers of shared data whom we do not trust.

The algorithm shown below is used for generating conflicting segments for controllers [2]. The policies of all controllers are used to derive the accessor space. The function named *Partition()* from line 10-28 in algorithm do the process. From the policies this function adds an accessor space s_a to an accessor space set AS. The lines from 5-9 identifies the conflicting segments.

Input : A group of accessor spaces, AS.

Output : A group of conflicting accessor spaces, CS which are disjoined

1. /*Partition the entire accessor space */
2. S= Partition (AS);
3. /*Identify the conflicting segments*/
4. CS. New();
5. for each s ∈ S do
6. /*Get all controllers associated with a segment s*/
7. C= GetControllers(s);
8. if $|C| < |AS|$ then
9. CS.Add(s);
10. Partition(AS);
11. for each a ∈ AS do
12. s_a = FriendSet(a);
13. for each s ∈ S do
14. /*s_a is a subset of s*/
15. if $s_a \subset s$ then
16. S. Add(s \ s_a);
17. s=s_a;
18. Break;
19. /*s_a is a superset of s*/
20. else if $s_a \supset s$
21. $s_a = s_a \setminus s$;
22. /*s_a partially matches s*/
23. else if $s_a \cap s \neq \emptyset$ then
24. S. Add(s \ s_a);

ISSN: 2278 – 7798

25. $s = s_a \cap s$;
26. $s_a = s_a \setminus s$;
27. S. Add(s_a);
28. return S;

Resolving Privacy Conflicts

For making a decision to permit or deny the accessors to access the shared data item within these identified conflicting segments we use the conflict resolution method. Privacy Risk is occurred when permitting the accessors in the conflicting segments to access the shared data item. While sharing loss is generated by denying a group of accessors in conflicting segments to access the shared data item. We must consider privacy protection and data sharing to find an ideal solution when resolving these conflicts.

Privacy Risk Estimation

The privacy risk of a conflicting segment is a measure of probable risk to the privacy of controllers associated with a particular shared data item. The higher the privacy risk of a conflicting segment, the higher the risk to controllers' privacy. For the measurement of privacy risk of a conflicting segment the elementary properties needed are: (a) the higher the privacy risk, the lower the number of controllers (b) the higher the privacy risk, the stronger the privacy concerns of the controllers (c) the higher the privacy risk, the shared data item is more sensitive (d) the higher the privacy risk, the data item spreads wider and (e) the higher the privacy risk, the lower the trust levels of accessors in the conflicting segment [4]. For a conflicting segment privacy risk is computed with certain factors like:

- **Number of untrusting controllers:** The number of untrusting controllers is equal to number of privacy conflicts. The untrusting controllers of a conflict segment *p* are returned by the function *getUntrustingControllers(m)*;
- **Privacy Concern of an untrusting controller:** The general privacy concern (pc_n) of an untrusting controller *j* is extracted from the privacy setting for sharing of data item. For the same data different controllers have dissimilar privacy concern. For example an eminent personality have higher privacy concern on their shared data item than a normal person;
- **Sensitivity of the data item:** Data sensitivity determines the confidentiality of shared data item. It is represented as sl_n.
- **Visibility of the data item:** The visibility of the data item in a conflicting segment denotes number of accessors in the segment. As the number of accessors in the conflicting segment increases the visibility all increases; and
- **Trust of an accessor:** The trust level (tl_a) of an accessor *a,* is a mean value of all the trust levels specified by the trusting controllers of the conflicting segment for the accessor.

The privacy risk due to an untrusting controller *n* of a conflict segment *m* is termed as controller risk and is defined by

$$\mathrm{CR}(m,n) = pc_n + sl_n + \sum_{a \in accessors(m)} (1 - tl_a)$$

where the function *accessors(m)* returns all accessors in a segment *m.*

For a conflicting segment the net privacy risk, PR(m) is calculated using the following equation:

$$PR(\mathrm{m}) = \sum_{n \in controllers(m)} (PR(m,n))$$

$$= \sum_{n \in controllers(m)} \left(pc_n * sl_n * \sum_{a \in accessors(m)} (1 - tl_a) \right)$$

This is used to find the gross privacy risks of *m* because of several untrusting controllers.

Sharing Loss Estimation:

Data sharing loss occurs due to the decision of privacy conflict resolution as "deny" for a conflicting segment while the controllers are ready to permit the accessors to access the shared data item in the conflicting segment. Sharing loss for a conflicting segment is obtained using five factors as in the case of privacy risk estimation [4]. Instead of using the factor, number of untrusting controllers here we use *number of trusting controllers* of a conflicting segment. The net sharing loss *SL*(*m*) of a conflicting segment *m* is calculated as:

$$\mathrm{SL}(m) = \sum_{n \in controllers(m)} \left((1 - pc_n * sl_n) * \sum_{a \in accessors(m)} (tl_a) \right)$$

where all trusting controllers of a segment *m* is returned by the function controllers (*m*).

Privacy Conflict Resolution

When permitting the accessors in conflicting segments to access the shared data item more privacy risk will occur in this ideal solution for privacy conflict resolution. And while denying accessors to access data it results in lesser loss.

In the privacy conflict resolution, to make a final decision, i.e. either permitting or denying conflicting segments we use the estimated privacy risk (*PR(m)*) and sharing loss (*SL(m)*) for each conflicting *m*. For making decision the equation used is:

$$Final\ Decision = \begin{cases} Permit, & if\ \alpha SL(m) \geq \beta PR(m) \\ Deny, & if\ \alpha SL(m) < \beta PR(m) \end{cases}$$

ISSN: 2278 – 7798

where, α and β are preference weights used for privacy risk and sharing loss, $0 \leq \alpha, \beta \leq 1$ and $\alpha + \beta = 1$.

IV. EXPERIMENTS AND RESULTS

In the system with multiparty access control mechanism, a set of users collude with one another to manipulate final decision. To evaluate our privacy conflict resolution method, we compare our solution with privacy control solution in existing OSNs, like Facebook with respect to privacy risk and sharing loss metrics. In Facebook solution, the highest priority is given to owner's decision. In our MPAC system the multiple controllers such as owner, contributor and stakeholder can make decision to on a single data whether it is made public or private.

Assume that there are 12 users. The given table shows the user id and id of friends in their profile.

TABLE FRIENDS LIST

User Id	Friends Id
1	2,3,5,7,9,13,14
2	1,5,6,8,11
3	1,4,9,10,13
4	3,9,10
5	1,2,8,11,12
6	2
7	1,15
8	2,5,11,12
9	1,3,4,10
10	3,4,9
11	2,5,8
12	5,8
13	1,3,14
14	1,13

Let the format of setting access control policy be (<controller id, controller type> || {accessor id: trust level: user name/group name>} || <owner id, sensitivity level>|| {Permit/Deny}).

Let the policy be {(5, CB), (2:1.0:UN; 1:0.5:UN; 12:1.0:UN),(1,1.0),permit}. Here the user5 (user id=5) post a data in the profile of user 11 and then set access such that the data can be viewed by users with id 1, 2 and 12.

Controller Id	Controller Type	Permitted Users	Trust Level	Sensitivity Level	Final Decision
5	CB	2 1 12	1.0 0.5 1.0	1.0	Permit Deny Deny

Now the owner of that data item is user 11. This user can further set access to the same data, so that permitted users can view it. Let that policy be {(11, OW), (8:0.25: UN), (1, 0.5), permit}.

Controller Id	Controller Type	Permitted Users	Trust Level	Sensitivity Level	Final Decision
11	OW	8	0.25	0.5	Permit

Let the policy be {(2, CB), (5:0.50: UN;6:0.0:UN; 1:1.0: UN; 8:0.75: UN), (7, 0.75), permit}. Here the user2 (user id=2) post a data in profile of user 5 and tagged users with id 5,6,1 and 8 and then set access such that the data can be viewed by users with id 1 and 8.

Controller Id	Controller Type	Permitted Users	Trust Level	Sensitivity Level	Final Decision
2	CB	5 6 1 8	0.5 0.0 1.0 0.75	0.75	Permit Deny Permit Permit

Now the owner of that data item is user 5. This user can further set access to the same data, so that permitted users can view it. Let that policy be {(5, SH), (12:0.25: UN ; 11:0.5:UN), (7, 0.75), permit}.

Controller Id	Controller Type	Permitted Users	Trust Level	Sensitivity Level	Final Decision
5	SH	12 11	0.25 0.50	0.75	Deny Permit

All these final decisions are made after checking whether there is any conflict between controllers of data. If there exists any conflict and have privacy risk with a particular user then access is denied, otherwise access is permitted. If the access is denied some loss in data sharing will be generated.

V. CONCLUSION

A multiparty access control model for collaborative management of shared data was developed with policy specification and evaluation scheme. The work provides a solution for privacy conflict detection and analyzed the power of MPAC conflict resolution method using the indicators like privacy risk and sharing loss. The users are involved in the privacy settings of large number of shared data item and its control are time consuming tasks. Additionally MPAC model provides decision voting scheme and evaluates privacy.

REFERENCES

[1] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms," IEEE Transactions, Vol 25, Issue 7, Pages 1614-1627, July 2013.

[2] H. Hu, G-J Ahn, and J.Jorgenson, "Detecting and resolving privacy Conflicts for collaborative data sharing in online social networks,"

ISSN: 2278 – 7798

[3] In Proceedings of the 27th Annual Computer Secutiry Applications Conference, ACSAC'11, pages 103-112, ACM, 2011.
[4] H. Hu, and G. Ahn, "Multiparty authorization framework for data sharing in online social networks," In Proceedings of the 25th annual IFIP WG 11.3 conference on Data and applications security and privacy, pages 29-43, Springer-Verlag, 2011.
[5] H.Hu, G.Ahn, and J.Jorgensen, "Enabling Collaborative Data Sharing in Google+," Technical Report ASU-SCIDSE-12-1, April 2012.
[6] 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
[7] 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.
[8] 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.
[9] Carminati and E.Ferrari, "Collaborative Access Control in Online Social Networks," IEEE, pages 231-240, 2011.
[10] Carminati, E.Ferrari, and A.Perego, "Rule-Based Access Control for Social Networks," Springer, pages 1734-1744, 2006.
[11] 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.
[12] Besmer and H.Ritcher Lipford, "Moving Beyond Untagging: Photoprivacy in a Tagged World," ACM, pages 1563-1572, 2010.
[13] H.Hu, G.Ahn, "Anomaly Discovery and resolution in web access control policies". In Proceedings of the 16th ACM symposium on Access control models and technologies, pages 165-174, ACM, 2011.

ISSN: 2278 – 7798