ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2014

Multiparty Access Control Model for Collaborative Management of Shared Data in Online Social Networks

K.B.Anusha[1], Dr.G.S.N.Murty[2]

[1]M.Tech Scholar, Department of Computer Science and Engineering, Aditya Institute of Technology and Management, Tekkali, Srikakulam (dt), A.P., India.

[2] Professor & Head, Department of Computer Science and Engineering, Aditya Institute of Technology and Management, Tekkali, Srikakulam (dt), A.P., India.

ABSTRACT: Online systems (OSNs) have perceived astounding advancement as of late and turn into a true webpage for toxic joined with online clients. These sorts of OSNs offer excellent opportunity for computerized friendly connections and additionally subtle elements uncovering, additionally hoist various insurance and also protection concerns. Despite the fact that OSNs let clients so as to minimize utilization of imparted data, these individuals at present tend not to supply essentially any system so as to put in power security contemplations around information identified with numerous clients. To this specific end, huge numbers of us propose a system for empower the genuine protection joined with imparted insight identified with various clients in OSNs. We deliver the induction administration demonstrate so as to seize the genuine quality joined with multiparty assent details, and additionally a multiparty scope principles framework in addition to a scope implementation component. Other than, a considerable lot of us present a practical representation of our own induction administration model which we can leverage the genuine top peculiarities of late reason solvers to execute various examination obligations with your model. We besides discuss a verification of idea model of our own methodology as a major aspect of a credit application in MySpace and still give ease of use research and system assess of our own strategy.

KEYWORDS: Social Network, Multiparty access control, Security model, Policy Specification and Management.

I. INTRODUCTION

Online Social Networks (OSNs) such as Facebook, Google+, and Twitter are inherently built to permit people to discuss private as well as community data as well as help make social internet connections together with good friends, co-workers, and colleagues, household and in some cases together with unknown people. Nowadays, we've got observed freakish progress within the application of OSNs. For example, MySpace, one among consultant online networks, statements so it has a lot more than eight hundred thousand productive end users as well as in excess of thirty million items of written content (web hyperlinks, news reports, web sites, paperwork, photograph for example.) discussed on a monthly basis. To safeguard person facts, accessibility manage has become a key feature regarding OSNs [1] [2].

A standard OSN gives each person having a digital space that contain report data, a summary of your user's good friends, as well as website pages, for instance wall structure within MySpace, wherever end users as well as good friends can certainly post written content as well as depart mail messages. The page typically incorporate data based on the user's birthday, sexuality, interests, and knowledge as well as operates history, as well as makes contact with data. Moreover, end users are unable to merely add any written content in very own or even others' rooms and also draw other end users exactly who can be purchased in necessary . Every single draw is surely a sometimes shocking guide that wills hyperlinks to a user's space. With the defense regarding person facts, current OSNs ultimately involve end users to be program as well as insurance plan staff for controlling their facts, wherever end users can certainly minimize facts expressing to a certain group of honest end users. OSNs usually make use of person marriage as well as

DOI: 10.15680/IJIRSET.2014.0309013

group membership to distinguish concerning honest as well as UN trusted end users. For example, within MySpace, end users can allow good friends; good friends regarding good friends, groups or even community gain access to their facts, based on their private consent as well as level of privacy specifications with respect to multiparty authorization in OSNs are also identified. Based on these sharing patterns, a multiparty access control (MPAC) model is 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 OSNs (e.g., [10]). Our model also contains a multiparty policy specification scheme. Meanwhile, since conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in our Model. An additional persuasive element your answer may be the service associated with examination on multiparty accessibility control model in addition to programs. This correctness associated with implementation of an accessibility control model is based on your assumption the accessibility control model will be appropriate.

II. RELATED WORK

MPAC model is formulated to capture the core features of multiparty authorization requirements that have not been accommodated so far by existing access control systems and models for OSNs. For this we used multiparty policy specification scheme. If a set of malicious users shares the photo which is available to a wider audience, they can access the photo, and then they tag themselves or making fake identities to the photo. So that they can assign a very low sensitivity level for the photo and also specify policies from users to access the photo. To prevent such an attack, three conditions should be satisfied: 1) There should not be any fake identity in OSNs; 2) Real user should be appeared in the photo when tagging is performed; and 3) all controllers of the photo should be honest by specifying their privacy preferences. For the first condition, Sybil attacks and Identity Clone attacks have been introduced to OSNs.

Regarding the second condition, an effective tag validation mechanism is used for verifying the tagged user against the photo. In this paper it tells that, if any users tag themselves or others in a photo then the photo owner will receive a tag notification. In such cases owner will come to know about the correctness of the tagged users. Facial recognition is used to recognize people accurately in contents such as photos, automatic tag validation is feasible. Regarding the third condition, it tells about the potential authorization impact with respect to a controller’s privacy preference. By using this function, the photo owner will examine the users who are granted to access the photo by the collaborative authorization which is not explicitly granted by the owner. Finally the owner can discover malicious activities in collaborative control.

Collusion detection in collaborative systems has been addressed by the recent work. Several access control models for OSNs have been introduced. Early access control solutions for OSNs introduced trust-based access control policy which is inspired by the development of trust and reputation computation in OSNs. Rule-based access control model for web based social networks allows the specification of access rules for online resources where authorized subjects are denoted in terms of the relationship type, depth, and trust level existing between users in the network. This is the first proposal of an access control model for social networks. The different tasks to be carried out to enforce access control are shared among three distinguished actors namely, the owner of the requested resource, the subject which requested it, and the SNMS. This paper allows us to associate with a relationship the users participating in it, its type, depth, and trust level.

III. MULTIPARTY ACCESS CONTROL FOR OSNS REQUIREMENTS AND PATTERNS

In this section we proceed with a comprehensive requirement analysis of multiparty access control in OSNs [9].
Meanwhile, we discuss several typical sharing patterns occurring in OSNs where multiple users may have different authorization requirements to a single resource. We specifically analyse three scenarios profile sharing, relationship sharing and content sharing to understand the risks posted by the lack of collaborative control in OSNs. We leverage Facebook as the running example in our discussion since it is currently the most popular and representative social network provider. In the meantime, we reiterate that our discussion could be easily extended to other existing social network platforms, such as Google+ [6].

DOI: 10.15680/IJIRSET.2014.0309013

3.1 Profile Sharing: A fascinating attribute connected with several OSNs is always to service interpersonal applications authored by third-party developers to produce added functionalities designed with top connected with users' report for OSNs [1], [5]. To supply meaningful along with beautiful solutions, these kinds of interpersonal applications ingest page capabilities, such as name, Birthday, things to do, likes and dislikes, and the like. To create issues harder, interpersonal applications about recent OSN systems could also ingest the report capabilities of the user's good friends. In such cases, users could pick distinct waste report capabilities that they are going to share with the applications as soon as his or her good friends make use of the applications. Concurrently, the users who definitely are when using the applications might also would like to handle what details in their good friends is available towards applications considering that you'll be able for that applications to be able to infer his or her exclusive report capabilities via his or her friends' report capabilities.

Which means as soon as a credit application accesses the report capabilities of the user's close friend, the consumer along with her close friend would like to attain handle within the report capabilities. In the event most of us find the software is definitely an accessor, an individual can be a disseminator along with the user's close friend are the owners of discussed report capabilities in this circumstance, Determine proves any report expressing pattern when a disseminator could share others' report capabilities to an accessor.

3.2 Relationship Sharing: Another characteristic connected with OSNs will be which customers may write about the romantic relationships along with additional members. Relationships usually are inherently bidirectional and take potentially sensitive data which affiliated customers might not wish to divulge. Nearly all OSNs present mechanisms which customers may control the screen in their buddy directories. A person, on the other hand, may merely control one route of any relationship. Allow us to consider, one example is, some sort of circumstances the place where a person Alice specifies a policy to cover the woman buddy listing from the open public. However, Bob, one of Alice's friends, specifies a weaker policy that permits his friend list visible to anyone. In this case, in the event that OSNs could exclusively apply just one party's plan, their bond involving Alice along with Bob could be learned through Bob's good friend listing. Determine it exhibits a new partnership sharing design certainly where a user called seller, who's a new partnership along with one more user called stakeholder, gives you their bond with the accessor.

3.3 Content Sharing: OSNs present built-in things enabling end users to help talk and also discuss articles having different members. OSN end users can easily submit statuses and also records, post photos and also movies into their very own spaces, tag people thus to their articles, and also discuss this articles using friends. Alternatively, end users also can submit articles into their friends' spaces. These discussed articles might be linked with a number of end users. Look at a case in point in which a photo is made up of several end users, Alice, Chad and also Carol. In case Alice uploads the idea to help her very own place and also labels the two Chad and also Carol in the photograph, most of us phone Alice the master of this photograph, and also Chad and also Carol stakeholders on the photograph. All of them may perhaps stipulate access handle guidelines to control more than who can view this photograph. Number describes any information discussing pattern wherever the master of any information gives you the content having different OSN members, and also the information offers a number of stakeholders exactly who may also need to contain in the handle connected with information discussing.

IV. MULTIPARTY ACCESS CONTROL MODEL FOR OSNS

In this section, we formalize a Multiparty Access Control (MPAC) model for OSNs (Section 4.1), as well as a policy scheme (Section 4.2) and a policy evaluation mechanism (Section 4.3) for the specification and enforcement of MPAC policies in OSNs.

4.1 MPAC Model: An OSN can be represented by a relationship network, a set of user groups and a collection of user data. The relationship network of an OSN is a directed labelled graph, where each node denotes a user and each edge represents a relationship between two users. The label associated with each edge indicates the type of the relationship. Edge direction denotes that the initial node of an edge establishes the relationship and the terminal node of the edge accepts the relationship. The number and type of supported relationships rely on the specific OSNs and its purposes. Besides, OSNs include an important feature that allows users to be organized in groups (or called circles in Google+ [6]

DOI: 10.15680/IJIRSET.2014.0309013

[8]), where each group has a unique name. This feature enables users of an OSN to easily find other users with whom they might share specific interests (e.g., same hobbies), demographic groups (e.g., studying at the same schools), political orientation, and so on. As we identified previously in the sharing patterns (Section 2), 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. 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 tagged users associated with d. A user u is called a stakeholder of d, if u2T.
Definition 4: (Disseminator). 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.

We now formally define our MPAC model as follows: Figure1 depicts an example of multiparty social network representation. It describes relationships of five individuals Alice (A), Bob (B), Carol (C), Dave (D) and Edward (E), along with their relations with data and their groups of interest. Note that two users may be directly connected by more than one edge labelled with different relationship types in the relationship network. Alice (A) has a direct relationship of type colleague Of with Bob (B), whereas Bob (B) has a relationship of friend Of with Alice (A). In addition, two users may have transitive relationship, such as friends-of-friends (FOF), colleagues-of-colleagues (COC) and classmates-of-classmates (LOL) in this example. Moreover, this example shows that some data items have multiple controllers. For instance, Relationship $_A$ has two controllers: the owner, Alice (A) and a stakeholder, Carol (C). Also, some users may be the controllers of multiple data items. For example, Carol (C) is a stakeholder of Relationship $_A$ as well as the contributor of Content. Furthermore, we can notice there are two groups in this example that users can participate in: the “Fashion” group and the “Hiking” group, and some users, such as Bob (B) and Dave (D), may join in multiple groups.

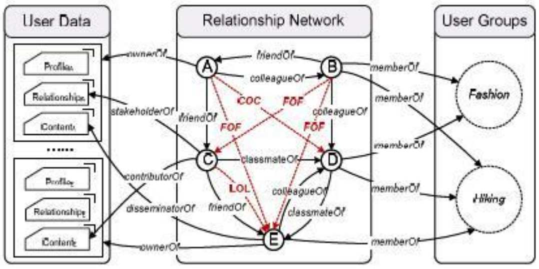


Fig.1 An Example of Multiparty Social Network Representation.

4.2 MPAC Policy Specification: Make it possible for some sort of collaborative agreement administration associated with data sharing with OSNs, it is necessary for multiparty gain access to management guidelines to stay destination for a determine gain access to more than contributed data, addressing agreement needs coming from multiple connected people. Our own insurance policy standards scheme is made on the particular recommended MPAC product.

A. Accessor Specification: Accessors are a set of people who definitely are granted to gain access to the shared info. Accessors might be showed with a collection of user brands, a collection of relationship brands or maybe a collection of collection brands in OSNs.
We formally define the accessor specification as follows:
Definition1 :(Accessor Specification). Let ac €u U RT U G be a user u€U, a relationship type rt € RT, or a group g€G. Let at€ {UN, RN, GN} be the type of the accessor specification (user name, relationship type, and group name, respectively). The accessor specification is defined as a set, accessors = {a_1. . . an$_}$, where each element is a tuple < ac, at >.

DOI: 10.15680/IJIRSET.2014.0309013

B. Data Specification: In OSNs, user data is composed of three types of information, user profile, user relationship and user content. To facilitate effective privacy conflict resolution for multiparty access control, we introduce sensitivity levels for data specification, which are assigned by the controllers to the shared data items. A user’s judgment of the sensitivity level of the data is not binary (private/public), but multi-dimensional with varying degrees of sensitivity. Formally, the data specification is defined as follows:

Definition 2: (Data Specification). Let dt € D be a data item. Let sl be a sensitivity level, which is a rational number in the range [0, 1], assigned to dt. The data specification is defined as a tuple <dt, sl>.
C. Access Control Policy: To summarize the above-mentioned policy elements, we introduce the definition of a multiparty access control policy as follows:
Definition3: A MPAC policy is a 5-tuple
P=<controller, ctype, accessor, data, effect>, where
a. controller € U is a user who can regulate the access of data;
b. ctype € CT is the type of the controller;
c. accessor is a set of users to whom the authorization is granted, representing with an access specification defined.
d. data is represented with a data specification defined in and
e. Effect € {permit; deny} is the authorization effect of the policy.

4.3 Policies
Sensitivity levels (SL) for data specification, which are assigned by the controllers to the shared data items. A user’s judgment of the SL of the data is not binary (private/public), but multidimensional with varying degrees of sensitivity. Suppose a controller can leverage five SLs: 0.00 (none), 0.25 (low), 0.50 (medium), 0.75 (high), and 1.00 (highest) for the shared data.

1. Voting Concept
Voting is a popular mechanism for decision making. A notable feature of the voting mechanism for conflict resolution is that the decision from each controller is able to have an effect on the final decision. Our voting scheme contains two voting mechanisms: decision voting and sensitivity voting.

A. Voting by decision
A decision voting value (DV) derived from the policy evaluation is defined as follows, where Evaluation (p) returns the decision of a policy p:

$$DV = \begin{cases} 0 & \text{if Evaluation(p) = Deny} \\ 1 & \text{if Evaluation(p) = Permit} \end{cases}$$

Assume that all controllers are equally important, an aggregated decision value (DV_{ag}) (with a range of 0.00 to 1.00) from multiple controllers including the owner (DV_{ow}), the contributor (DV_{cb}) and stakeholders (DV_{st}), is computed with following equation:

$$DV_{ag}=(DV_{ow}+DV_{cb}+\sum_{i€SS} DV^{i}_{st})X1/m$$

Where SS is the stakeholder set of the shared data item, and m is the number of controllers of the shared data item. Each controller of the shared data item may have 1) a different trust level over the data owner and 2) a different reputation value in terms of collaborative control [7].Thus, a generalized decision voting scheme needs to introduce weights, which can be calculated by aggregating trust levels and reputation values, on different controllers. Different weights of controllers are essentially represented by different importance degrees on the aggregated decision. In general, the importance degree of controller x is

$$DV_{ag} = (w_{ow} \times DV_{ow} + w_{cb} \times DV_{cb} + \sum_{i=1} (w_{st}^{i}\ DV_{st}^{i})) \times (1/w_{ow} + w_{cb} + \sum^{n}_{i=1} w_{st}^{i})$$

B. Voting using sensitivity level: Each controller assigns an SL to the shared data item to reflect her/his privacy concern. A sensitivity score (Sc) (in the range from 0.00 to 1.00) for the data item can be calculated based on following equation:

$$SC= (SL_{ow} + SL_{cb} +\sum_{i€ss} SL^{i}_{st})X1/m$$

C. Threshold-based concept: A basic idea of our approach for threshold-based conflict resolution is that the Sc can be utilized as a threshold for decision making. Intuitively, if the Sc is higher, the final decision has a high chance to deny access, taking into account the privacy protection of high sensitive data.

$$\text{Decision}= \begin{cases} \text{Permit if } DV_{ag} > SC \\ \text{Deny if } DV_{ag} \leq SC \end{cases}$$

3. Strategy-based concept

a. Owner overrides: The owner's decision has the highest priority. This strategy achieves the owner control mechanism that most OSNs are currently utilizing for data sharing. Based on the weighted decision voting scheme, we set , =0and = and the final decision can be made as follows:

$$\text{Decision}= \begin{cases} \text{Permit if } DVag = 1 \\ \text{Deny if } DVag = 0 \end{cases}$$

b. Full consensus permit: If any controller denies the access, the final decision is deny. This strategy can achieve the naive conflict resolution that we discussed previously. The final decision can be derived as:

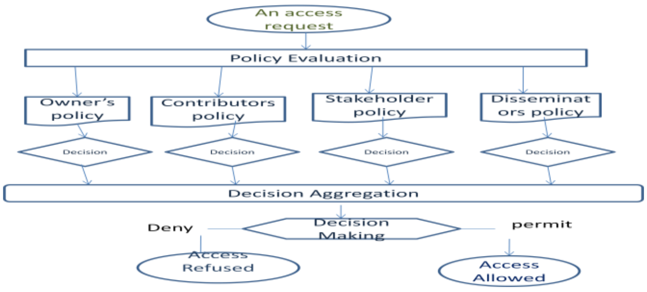
$$\text{Decision}= \begin{cases} \text{Permit if } DVag = 1 \\ \text{Deny Otherwise} \end{cases}$$

c. Majority permit: This strategy permits (deny, resp.) a request if the number of controllers to permit (deny, resp.) the request is greater than the number of controllers to deny (permit, resp.) the request. The final decision can be made as

$$\text{Decision}= \begin{cases} \text{Permit if } DV_{ag} \geq 1/2 \\ \text{Deny if } DV_{ag} < 1/2 \end{cases}$$

4.4 Multiparty Policy Evaluation:

Two steps are performed to evaluate an access request over multiparty access control policies. The first step checks the actual gain access to request against the insurance policy specified simply by every controller and brings a conclusion with the controller. Two steps are performed to evaluate an access request over multi- party access control policies. The first one checks the access request against the policy specified by each controller and yields a decision for the controller. The accessor element in a policy decides whether that policy is applicable to a request and returns a response with the decision (either permit or deny), Otherwise, the response yields deny decision if the policy is not applicable to that request. In the second one, decisions from all controllers responding to the access request are aggregated to make a final decision for the access request. Figure 2 illustrates the evaluation process of multi- party access control policies



.

Fig.2 Multiparty Policy Evaluation Process

DOI: 10.15680/IJIRSET.2014.0309013

V. IMPLEMENTATION

A. Processing of social networks: Users upload the photo in their own space and tags to their friends, and the owner of the photo will be the uploaded person, and stakeholders of the photo will be the tagged members. All users can specify access control policies to control over the photo and can see the photo. OSNs also enable users to share others' contents. To view a photo in friend's space and decide to share that photo with our friends, the photo will be in turn posted in their space and can specify access control policy to authorized friends to see that photo. In such cases, the person is a disseminator who shared their friend's photo.

B. Features of Online Social Network's: When user uses the social applications, they want to control what information about their friends is available in the applications. It is also possible for the social applications to infer their private profile attributes through their friends' profile attributes. When social application accesses the profile attributes of a user's friend, and also both the user and her friend want to gain control over the profile attributes. Consider the application is an accessor, the user is a disseminator, and the user's friend is the owner of shared profile attributes in this scenario, a profile sharing pattern where a disseminator can share others' profile attributes to an accessor. Here the owner as well as the disseminator can specify access control policies by restricting the sharing of profile attributes.

User is able to control one direction of a relationship. In relationship sharing pattern, a user is said to be owner, who has a relationship with another user called stakeholder, and shares the relationship with an accessor. In this concept, authorization requirements from both the owner and the stakeholder should be considered. Or else the stakeholder's privacy concern may be violated Multiparty access control model is formulated to capture the core features of multiparty authorization requirements that have not been accommodated so far by existing access control systems and models for OSNs. In this model multiparty policy specification scheme is used. Since conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in our model. Another compelling feature of our solution is the support of analysis on the MPAC model and systems.

C. Objective: The main objective of this paper tells about Multiparty Access Control mechanisms greatly enhance the flexibility for data sharing in OSNs. It may potentially reduce the certainty of system authorization consequences so that authorization and privacy conflicts can be resolved elegantly. Additionally introduce a method to represent and reason about our model in a logic program. In addition, a prototype implementation of our authorization mechanism in the context of Facebook has been introduced. Experimental results demonstrate the feasibility and usability of our approach. Multiparty authorization requirements and access control patterns for OSNs are used [10].

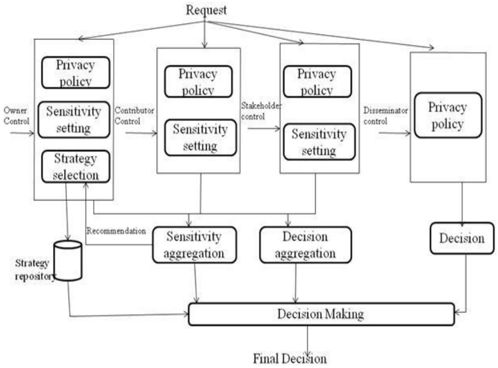


Fig. 3 Architecture Diagram

A core component of MController is the decision making module, which processes access requests and returns responses (either permit or deny) for the requests. Figure4 depicts system architecture of the decision making module in MController. To evaluate an access request, the policies of each controller of the targeted content are enforced first to generate a decision for the controller. Then, the decisions of all controllers are aggregated to yield a final decision as

DOI: 10.15680/IJIRSET.2014.0309013

the response of the request. Multiparty privacy conflicts are resolved based on the configured conflict resolution mechanism when aggregating the decisions of controllers. If the owner of the content chooses automatic conflict resolution, the aggregated sensitivity value is utilized as a threshold for decision making. Otherwise, multi-party privacy conflicts are resolved by applying the strategy selected by the owner, and the aggregated sensitivity score is considered as a recommendation for strategy selection. Regarding the access requests to disseminated content, the final decision is made by combining the disseminator's decision and original controllers' decision adopting corresponding combination strategy discussed previously.

VI. SYSTEM USABILITY AND PERFORMANCE EVALUATION

6.1 Participants and Procedure:

MController is a functional proof-of-concept implementation of collaborative privacy management. To measure the practicality and usability of our mechanism, we conducted a survey study (n=35) to explore the factors surrounding users' desires for privacy and discover how we might improve those implemented in MController. Specifically, we were interested in users' perspectives on the current Facebook privacy system and their desires for more control over photos they do not own. We recruited participants through university mailing lists and through Facebook itself using Face book's built-in sharing API. Users were given the opportunity to share our application and play with their friends. While this is not a random sampling, recruiting using the natural dissemination features of Facebook arguably gives an accurate profile of the ecosystem.

6.2 User Study of MController:

For evaluation purposes, questions were split into three areas: likeability, simplicity, and control. Likeability is a measure of a user's satisfaction with a system Simplicity is a measure how intuitive and useful the system is (e.g. "Setting my privacy settings for a photo in MController is Complicated (1) to Simple (5)" with a 5-point scale). Control is a measure of the user's perceived control of their personal data (e.g. "If Facebook implemented controls like MController's to control photo privacy, my photos would be better protected"). Questions were either True/False or measured on a 5-point likert scale, and all responses were scaled from 0 to 1 for numerical analysis.

TABLE 1

Usability Evaluation for Facebook and MController Privacy Controls.

Metric	Facebook		MController	
	Average	Upper bound on 95% confidence interval	Average	Lower bound on 95% confidence interval
Likability	0.20	0.25	0.83	0.80
Simplicity	0.38	0.44	0.72	0.64
Control	0.20	0.25	0.83	0.80

VII. CONCLUSION

Multiparty Access Control Model has been formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism to provide a novel solution for collaborative management of shared data in OSNs. We would study inference-based techniques for automatically configure privacy preferences in MPAC. Besides, we plan to systematically integrate the notion of trust and reputation into our MPAC model and investigate a comprehensive solution to cope with collusion attacks for providing a robust MPAC service in OSNs.

DOI: 10.15680/IJIRSET.2014.0309013

REFERENCES

1. 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.
2. Carminati and E. Ferrari, Collaborative access control in on-line social networks. In *Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing (CollaborateCom)*, pages 231–240, IEEE, 2011.
3. 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 Applications Conference*, ACSAC '11, pages 103–112, ACM, 2011.
4. 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
5. L. Jin, H. Takabi, and J. Joshi, towards active detection of identity clone attacks on online social networks. In *Proceedings of the first ACM conference on Data and application security and privacy*, pages 27–38, ACM, 2011.
6. 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. Carrie, Access Control Requirements for Web 2.0 Security and Privacy, In Proc. of Workshop on Web 2.0 Security & Privacy (W2SP), Citeseer, 2007.
9. L. Fang and K. LeFevre, Privacy wizards for social networking sites, In Proceedings of the 19th international conference on World Wide Web, pages 351–360. ACM, 2010.
10. N.Li and M.Tripunitara, Security analysis in role-based access control, *ACM Transactions on Information and System Security (TISSEC)*, 9(4):391–420, 2006.

DOI: 10.15680/IJIRSET.2014.0309013