Security Features of User's for Online Social Networks

A. Radha Krishna*
K. Chandra Sekharaiah**

Abstract

In recent years Online social networks (OSNs) have practiced fabulous growth and become a genuine portal for hundreds of millions of Internet users. These OSNs provides attractive ways for digital social interactions and information sharing, but also raise a number of security and privacy issues. OSNs allow users to control access to shared data, they currently do not provide any method to enforce privacy concerns over data connected with multiple users.To this end, we suggest an progress to enable the protection of shared data associated with multiple users in OSNs. . We formulate an access control model to capture these sense of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, we present a logical representation of our access control model that allows us to influence the features of existing logic solvers to perform various analysis tasks on our model. We also discuss a proof-of-concept prototype of our approach as part of an application in Facebook and provide usability study and system evaluation of our method.

Keywords: Multiparty Access Control, Multiparty Policy, Online Social Network

Introduction

Motivation

The motivation for writing this paper is primarily an interest in undertaking a challenging task in an interesting area of research (Networking). The opportunity to learn about a new area of computing not covered in lectures.

Problem Definition

The rising of the technology made the communication more easier for the people who are far from us by communicating through the social networks like Facebook, twitter etc., These social networks are mainly used for different activities such as education, business, entertainment etc., But using these social networks there are some troubles like security, privacy etc.

Several benefits of this paper introduces are cut detection capability, suppose if a sensor wants to send data to the source node has been disconnected from the source node. Without the knowledge of the network's disconnected state, it may simply forward the data to the next node in the routing tree, which will do the same to its next node, and so on. However, this message passing merely wastes precious energy of the nodes; the cut prevents the data from reaching the destination.

Therefore, on one hand, if a node were able to detect the occurrence of a cut, it could simply wait for the network to be repaired and eventually reconnected, which saves on board energy of multiple nodes and prolongs their lives. On the other hand, the ability of the source node to detect the occurrence and location of a cut will allow it to undertake network repair.

Thus, the ability to detect cuts by both the disconnected nodes and the source node will lead to the increase in the operational lifetime of the network as a whole.

Objective of the Paper

- Platforms are allowing people to publish their details about themselves and to connect to other members of the network through links so now a days Online Social Networks (OSNs) are becoming more popular eg: Facebook used by hundred million active users.

A. Radha Krishna*
vasjrs2004@gmail.com

K. Chandra Sekharaiah**
chandrasekharaiahk@gamil.com

- The subsistence of OSNs that include person specific information creates both interesting opportunities and challenges.
- On the other hand, simply making a user able to decide which personal information are accessible by other members by marking a given item as public, private, or accessible by their direct contacts by very basic access control systems of current OSNs put into service .
- In order to provide more flexibility, some online social networks implement variants of these settings, but the principle is the same.

Objectives

a. Safety measure policies.

b. Unconstitutional access control

c. To identify their permission provide policy and privacy for multiple user

d. Discover potential nasty activities using collaborative control

e. An Online Social Network with User- Defined Privacy.

Literature Survey

- Online Social Networks (OSNs) have seen major growth and are getting much consideration in research in recent years. Social Networks have always been an important part of daily life.
- Because of the public nature of many social networks and the Internet itself, content can easily be disclosed to a wider audience than the user intended. Limited experience and awareness of users, as well as the lack of proper tools and design of the OSNs, do not help the situation. We feel that users are entitled to at least the same level of privacy in OSNs, that they enjoy in real life interactions. Users should be able to trade some information for functionality without that information becoming available beyond the intended scope. For example, a user of a self-help OSN like Patients-Like-Me, who suffers from a given medical condition might not want everyone to know about this, but at the same time the user would like to meet people with the same condition. This is the context of the Kindred Spirits project, and its aim is to provide users the ability to meet and interact with other (similar) people, while preserving their privacy. This project aims to provide insight into privacy issues and needs faced by users of OSNs and their origins. The insights gained help plot a course for future work. To this end, we look at OSNs as they currently exist, the associated privacy risks, and existing research into solutions. The ultimate goal is to identify open topics in research through reflection on existing proposals.

Online Social Networks

Let the concept begins with the Online Social Networks and why it becoming more popular today. This will help us understand the needs of OSN. Users environments they navigate, and potential threats are discussed in further sections.

Definition Of OSNs

Boyd and Ellison's widely used definition captures the key elements of any OSN: Definitions

1. An OSN is a web-based service that allows individuals to:

1. Construct a public or semi-public profile within the service,
2. Articulate a list of other users with whom they share a connection,
3. View and traverse their list of connections and those made by others within the service.

The list of other users with whom a connection is shared is not limited to connections like friend (Facebook, MySpace) or relative (Genie), but also includes connections like follower (Twitter), professional (Linked In) or subscriber (YouTube).

Types of OSNs

Classification of OSNs based on the openness of the network, we will look at the purpose or functionality that an OSN aims to offer to its user base.

- **Connection OSNs: :** Connection OSNs focus more on the connecting users and by providing a social contact book.
- **Business:** These OSNs aim to provide professionals with useful business contacts,

searching for profiles does not always require signing up. Profiles display a users capabilities and work field, this is based on the OSN via messages. This also provide the facility to user to add other user to their network,so that the professional can see whether the user is working or not.

- **Enforcing real-life relationships**: These OSNs are not aimed at finding new friends, but (re)connecting with existing friends or acquaintances that are far.
- **Socializing**: Fitting the more traditional view of social networks. Here users can connect with current friends and find new ones. All types of information found in an OSN are also found in this class; often a lot of this information is public. In order to keep the users this type of OSNs are providing the competitive and social games. Some well known examples of this class are Hypes, Facebook, Orkut and MySpace.
- **Content OSNs:** Content OSNs focus more on the content provided or linked to by users.
- **Content Sharing**: Sharing of user-generated content within a selected group, such as friends or family, or a far wider audience. Content that is shared is usually multimedia. Uploading content most often requires users to sign up and log in; sometimes viewing content also requires logging in, or knowledge of a hard-to-guess obfuscated URL.Examples are Picasa and Photo bucket
- **Content recommendation**: In some cases users do not upload (multimedia) content, but focus more on recommending existing (usually professional) content. Some Book review sites like We Read.com, and URL-tagging communities like Delicious are prime examples where content is discovered and tagged or rated, but not created or uploaded.
- **Entertainment:** These OSNs are tied to a gaming community. Entertainment OSNs might make money by selling games and game add-ons, or through subscriptions. Examples are Xbox.Live and Play fire.

Table 1: Data Types Typically Found in Different of OSNs

↓ OSN types	Data types →	Profiles	Connections	Messages	Multi-media	Tags	Preferences	Groups	Behavioral information	Log in credentials
Connection OSNs	Dating	●	•	●	•	-	●	•	●	●
	Business	●	●	●	•	-	•	●	●	●
	Enforcing real-life relationships	●	●	●	•	-	•	●	●	●
	Socializing	●	●	●	•	-	•	●	●	●
Content OSNs	Content sharing	•	•	●	●	●	•	•	●	●
	Content recommendation	●	-	•	●	●	●	•	●	●
	Entertainment	•	•	●	●	•	●	●	●	●
	Advice sharing	●	•	●	•	•	•	●	●	●
	Hobbies	•	•	●	•	•	•	●	●	●
	"News" sharing	•	•	●	●	•	•	•	●	●

Fig. 1 Multiparty Policy Evalution

- **Advice sharing:** place for people to share their experience or expertise in a certain area with others,and advice can be a focus for some OSNs. For example mothers-to-be (Baby Center), medical patients (PatientsLikeMe) or students (Teach Street) can help one another.
- **Hobbies**: Many OSNs focus on audiences that have similar interests and hobbies. This may involve advice sharing elements,but the audience is more homogenous.Examples are Athelings and Care2. "News" sharing. Blog-related OSNs, or ones that focus on world news or gossip. Examples are Buurtlinknl, Twitter, Blogster and GossipReport.com.

Multiparty Policy Evaluation

Two steps are performed to evaluate an access request over MPAC policies.

- The first step 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 the policy is applicable to a request or not.If the user who send the sends the request belongs to the user set derived from the accessor of a policy, the policy is applicable and the evaluation process returns a response with the decision (either permit or deny) indicated by the effect element in the policy. Otherwise, the response yields deny decision if the policy is not applicable to the request.
- In the second step, decisions from all controllers responding to the access request are aggregated to make a final decision for the access request. Fig. 1 illustrates the evaluation process of MPAC policies.

Since data controllers may generate different decisions (permit and deny) for an access request, conflicts may occur.

A Voting Scheme for Decision Making of Multiparty Control

Voting scheme to achieve an effective multiparty conflict resolution for OSNs. 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. Majority voting is a popular mechanism for decision making, Decision voting.

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= { 0 if Evaluation(p)deny
1 if Evaluation(p) Permit

Assume that all controllers are equally important, an aggregated decision value (DVag)(with a range of 0.00 to1.00) from multiple controllers including the owner (DVow),the contributor (DVcb), and stakeholders (DVst) is computed with following equation:

$$DV_{ag} = \left(DV_{ow} + DV_{cb} + \sum_{i \in SS} DV_{st}^{i} \right) \times \frac{1}{m},$$

where 'SS' is the stakeholder set of the shared data item, and m is the number of controllers of the shared data item.

Sensitivity voting. 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:

$$\mathrm{Sc} = \left(SL_{ow} + SL_{cb} + \sum_{i \in SS} SL_{st}^{i} \right) \times \frac{1}{m}.$$

Threshold-based Conflict Resolution

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.

Otherwise, the final decision is very likely to allow access, so that the utility of OSN services cannot be affected. The final decision is made automatically by OSN systems with this threshold-based conflict resolution as follows:

$$Decision = \begin{cases} \text{Permit} & \text{if } DV_{ag} > \mathrm{Sc} \\ \text{Deny} & \text{if } DV_{ag} \leq \mathrm{Sc}. \end{cases}$$

It is worth noticing that our conflict resolution approach has an adaptive feature that reflects the changes of policies and SLs. If any controller changes her/his policy or SL for the shared data item, the DVag and Sc will be recomputed and the final decision may be changed accordingly.

Strategy-based Conflict Resolution with Privacy Recommendation

In this conflict resolution, the Sc of a data item is considered as a guideline for the owner of shared data item in selecting an appropriate strategy for conflict resolution. We introduce following strategies for the purpose of resolving multiparty privacy conflicts in OSNs:

- Owneroverrides: 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 $\omega_{ow} = 1$, $\omega_{cb} = 0$, and $\omega_{st} = 0$,[1] and the final decision can be made as follows:

$$Decision = \begin{cases} \text{Permit} & \text{if } DV_{ag} = 1 \\ \text{Deny} & \text{if } DV_{ag} = 0 \end{cases}$$

- Fullconsensuspermit: 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:

$$Decision = \begin{cases} \text{Permit} & \text{if } DV_{ag} = 1 \\ \text{Deny} & \text{otherwise.} \end{cases}$$

- Majoritypermit: This strategy permits (denies, 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

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

Other majority voting strategies can be easily supported by our voting scheme, such as strong-majority permit (this strategy permits a request if over two-third controllers permit it), super-majority-permit (this strategy permits a request if over three-fourth controllers permit it).

Logical Definition of Multiple Controllers and Transitive Relationships

The basic components and relations in our MPAC model can be directly defined with corresponding predicates in ASP. We have defined UD_{ct} as a set of user-to-datarelations with controller type $ct \in CT$. Then, the logical definition of multiple controllers is as follows:

The owner of a data item can be represented as:

$$OW(controller, data) \leftarrow UD_{OW}(controller, data) \wedge U(controller) \wedge D(data).$$

The contributor of a data item can be represented as:

$$CB(controller, data) \leftarrow UD_{CB}(controller, data) \wedge U(controller) \wedge D(data).$$

The stakeholder of a data item can be represented as:

$$ST(controller, data) \leftarrow UD_{ST}(controller, data) \wedge U(controller) \wedge D(data).$$

The disseminator of a data item can be represented as:

$$DS(controller, data) \leftarrow UD_{DS}(controller, data) \wedge U(controller) \wedge D(data).$$

Our MPAC model supports transitive relationships. For example, David is a friend of Allice, and Edward is a friend of David in a social network. Then, we call Edward is a friends of friends of Allice. The friend relation between two users Allice and David is represented in ASP as follows:

$$friendOf(Allice, David).$$

It is known that the transitive closure (e.g., reachability) cannot be expressed in the first order logic [33]; however, it can be easily handled in the stable model semantics. Then, FOF can be represented as a transitive closure of friend relation with ASP as follows:

$$friendsOFfriends(U1, U2) \leftarrow friendOf(U1, U2).$$
$$friendsOFfriends(U1, U3) \leftarrow friendsOFfriends(U1, U2), friendsOFfriends(U2, U3).$$

Example : (Checking Undersharing). Bob has defined a policy to authorize his friends to see a photo. He wants to check if any friends cannot see this photo in current system. The input query Π_{query} can be specified as follows:

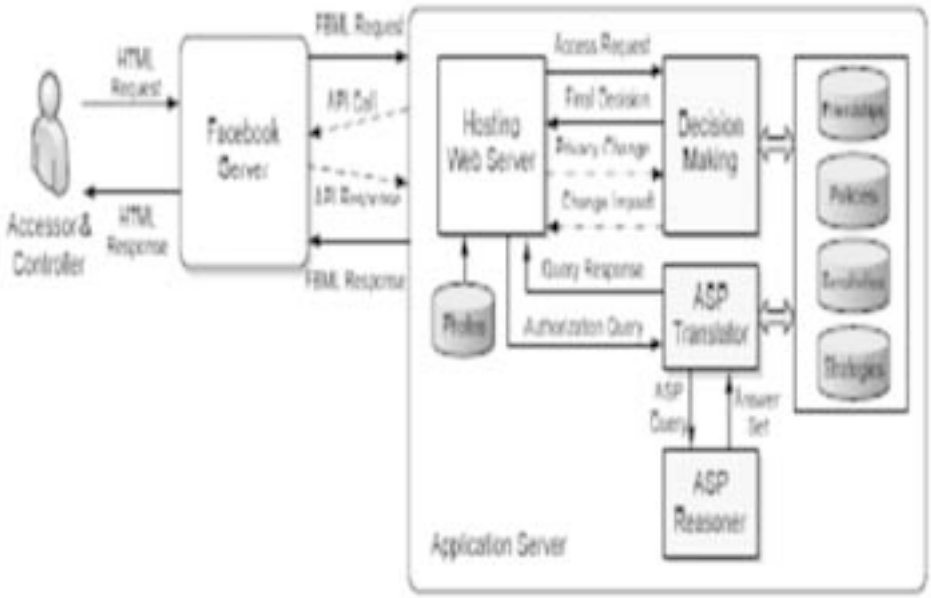

Fig. 2. Overall Architecture of MController Application

check:-decision(deny),friendof(bob,x),
ow(alice,photoid),user(bob),
user(x),photo(photoid).
:-notcheck.

If an answer set contains check, this means that there are friends who cannot view the photo. Regarding Bob's authorization requirement, this photo is under shared with his friends.

Implementation and Evaluation

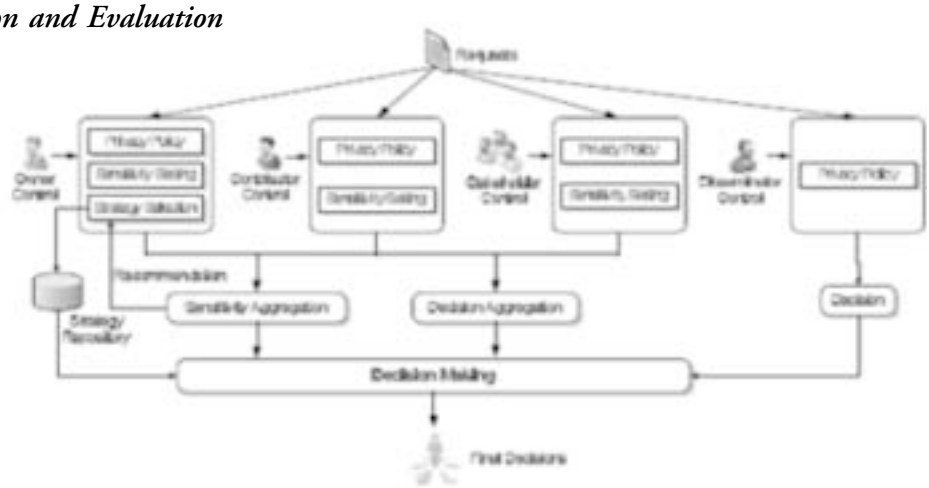

Fig. 3 System Architecture of Decision

Making in Mcontrloller

A 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 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, multiparty privacy conflicts are resolved by applying the strategy selected by the owner, and the aggregated Sc 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.

System Usability and Performance Evaluation

Proposed System

Our solution is to support the analysis of multiparty access control model and mechanism systems. The use

Table-2: Usability Study 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

of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in Online social networks (OSNs),it may reduce the privacy conflicts need to be resolved sophisticatedly.

The following are scenario like content sharing to understand the risks posted by the lack of collaborative control in online social networks (OSNs).

Proposed System Advantages:

- It checks the access request against the policy specified for every user and yields a decision for the access.
- The use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in online social networks.
- Present any mechanism to enforce privacy concerns over data associated with many users.
- If a user posts a comment in a friend's space, he/she can specify which users can view the comment.

Conclusions

In this paper, in OSNs we have proposed a novel solution for collaborative management of shared data. An MPAC model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model. A proof-of-concept implementation of our solution called MController has been discussed as well, followed by the usability study and system evaluation of our method.

As part we are planning to examine more comprehensive privacy conflict resolution approach and analysis services for collaborative management of shared data in OSNs in future work. Also, we would search more criteria to estimate the features of our proposed MPAC model. For example, one of our recent work has evaluated the effectiveness of the MPAC conflict resolution approach based on the tradeoff of privacy risk and sharing loss. In addition, users may be involved in the arrangements of the privacy preferences may become time consuming and tedious tasks and control of a larger number of shared photos.Therefore, we would study inference-based techniques for automatically configure privacy preferences in MPAC. Besides, we plan to thoroughly integrate the notion of trust and reputation into our MPAC model and examine a comprehensive solution to cope with collusion attacks for providing a robust MPAC service in OSNs.

References

1. FacebookDevelopers,http://developers.facebook.com/, 2013.
2. FacebookPrivacyPolicy,http://www.facebook.com/policy.php/, 2013.
3. FacebookStatistics, http://www.facebook.com/press/info. php?statistics, 2013.
4. Google+PrivacyPolicy,http://http://www.google.com/intl/en/+/policy/, 2013.
5. The Google+ Project, https://plus.google.com, 2013.
6. G. Ahn and H. Hu, "Towards Realizing a Formal RBAC Model in Real Systems," Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 215-224, 2007.
7. G.Ahn, H.Hu, J. Lee, and Y. Meng, "Representing and Reasoning about Web Access Control Policies," Proc. IEEE 34th Ann. Computer Software and Applications Conf. (COMPSAC), pp. 137-146, 2010.
8. A. Besmer and H.R. Lipford, "Moving beyond Untagging: Photo Privacy in a Tagged World," *Proc. 28th Int'l Conf. Human Factors in Computing Systems,*pp. 1563-1572, 2010.
9. L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All Your Contacts Are Belong to Us: Automated Identity theft Attacks on Social Networks," *Proc. 18th Int'l Conf. World Wide Web*, pp. 551-560, 2009.
10. B. Carminati and E. Ferrari, "Collaborative Access Control in OnLine Social Networks," *Proc. Seventh Int'l Conf. Collaborative Computing: Networking, Applications and Worksharing* (Collaborate-Com), pp. 231-240, 2011.
11. B. Carminati, E. Ferrari, and A. Perego, "Rule-Based Access Control for Social Networks," *Proc. Int'l Conf. On the Move to Meaningful Internet Systems*, pp. 1734-1744, 2006.