A Comparative Analysis of the Social Graph Model and Multiparty Access Control Model for Online Social Networks

Gabriela Suntaxi-Oña and Vijay Varadharajan

***Abstract*—In recent years, with the growth of the Internet, the number of users of Online Social Networks (OSNs) has increase. Users use these systems to communicate and share information with each other. In order to protect the amount of data that is being shared in these systems and to avoid security and privacy issues, it is important to have an adequate Access Control Model. Researchers have proposed different access control models to satisfy users' requirements and address the security and privacy issues. This paper presents a discussion of strength and weaknesses of the Social Graph Model and Multiparty Access Control Model. In addition, we provide a comparative analysis of the selected models based on the access control requirements with the purpose of determining whether the models fulfill or not the social requirements of the community.**

***Index Terms*—Access control model, online social network, security model, policy specification.**

I. Introduction

An Online Social Network is a network composed by users that can be represented by persons, groups or organizations, who establish different types of relationships with other users in order to interact between them, share information, resources and more. When a user decides to register to an OSNs system, it gives him an account; which consists on a profile where the user can upload photos, videos, documents, personal information and specify his relationship with other users [1], [2]. Depending on the system, the user is also able to manage his resources and information and decide who can access them. In order to protect this tremendous amount of data and avoid security issues, OSNs must provide users an adequate access control over their resources and the users who can access them, having on mind that users typically do not want to share their information with everyone.

An effective access control model has to protect all this information and resources from unauthorized access in OSNs

Let us consider a Social Network scenario, to understand the functionality, main features of these systems and the role that access control models play to protect users' privacy. The scenario is based on the sample social graph displayed on Fig. 1. Alice is an OSN's user. As a user, she has a profile and she decides to upload a photo on this. In this scenario, Alice is the owner of the photo and the photo uploaded is considered her resource. As the owner user, she wants to have control over her resource in order to regulate the access to it. An access control policy defines who can access what resource. Thus, Alice states the policies and establishes that her friends can access her photo. The OSN system's function is to protect Alice's resource, allowing that only users that have been granted authority can access it. In this scenario, as Alice knows her friends, she is able to establish a set of policies to grant access to her photo only to her friends. In a more general scenario, Alice wants to share her resource not only with her friends but also with her friends of friends. As Alice does not know her indirect friends she is not able to specify a set of policies that apply only to them. Even if she knew all of her indirect friends, she will need to specify a huge number of policies for all of them. Also it is important to consider that these relationships could change dynamically over the time. An access control model for OSNs needs to consider that users want to share their resources with other users based on the type of relationships that they share.

Recent related studies [1], [3]-[5] reveal that: Privacy settings are inconsistent with users' sharing intentions, numerous features of social networks have not been implemented yet and there is a gap between social requirements and access control models for OSNs. Therefore, a study of the existing and relevant access control models is needed to determine the current state of art of the Access Control Models in OSNs.

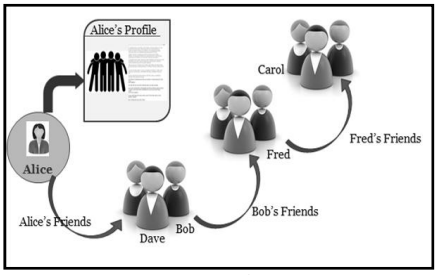

Fig. 1. A social graph of an OSN system.

The reminder of this document is organized as follows. First, we determine the access control requirements for OSNs in Section II. Then, we present a study of the existing and relevant access control models in Section III. In this section, we review the main features of the models. Also, the expressiveness of each access control scheme is presented through real life scenarios. To finalize this section, we present a discussion with the strengths and weaknesses of each scheme.

Section IV includes a comparative analysis of the schemes selected for this study based on the requirements established on Section II. Finally, in Section V we outline some future

Manuscript received March 5, 2015; revised September 28, 2015.

Gabriela Suntaxi-Oña is with the Department of Informatics and Computer Science of the National Polytechnic School, Quito, Ecuador (e-mail: gabriela.suntaxi@epn.edu.ec).

Vijay Varadharajan is with the Department of Computing, Macquarie University, Sydney, Australia (e-mail: vijay.vharadarajan@mq.edu.ec).

doi: 10.18178/ijfcc.2015.4.5.404

work and conclude the paper.

II. Access Control Requirements for OSNs

Although OSN systems provide users simple mechanisms to configure who can access their resources, access control policies are considered difficult to configure adequately in order to match with users' sharing intentions [3], [6]. Therefore, it is important to specify the requirements that these system should fulfill.

In this section we identify and proceed with a comprehensive analysis of the essential characteristics and requirements that need to be addressed by OSN access control models based on the requirements of the community. We categorize the access control requirements identified in these systems in three major groups based on their characteristics. We recognize access control requirements based on the point of view of the user and the source that is going to be accessed. The next group was identified based on the point of view of who manages the OSN system. This section finalize by looking at the access control requirements from the point of view of features offered by the OSN system to the users in order to fulfill certain needs.

First, let us look at the access control requirements from the point of view of the user and the source that is going to be accessed. We identify six requirements.

A. Requestor Identity

In Social Networks, requestor identity addresses how the users create relationships with other users and how friends are identified in the social graph. Similar mechanisms to this one are Access Control Lists and Capabilities.

B. Mapping Authority

In order to access a resource, the requestor users need to have a relationship with the resource's owner. This mapping of the relationship between them is done by the mapping authority. There are different types of mapping authorities: Owner, System [7] and the Community.

C. User and Resource as a Target

Access control models for OSNs differ from traditional ones because it is necessary to establish policies not only for access resources but also for interacting with users. For instance, activities such as: tag a user in a photo, poke or recommend a friend to another user require policies to carry out these actions. Thus, users as well as resources need to be considered as targets.

D. Policy Individualization

This requirement expresses that each user needs to express his own access control policies for his resources; which is considered a significant feature by users in OSN systems. The aim of the OSN system is to collect individual policies from the users related with a resource in order to take an access control decision.

E. Relationship-Based

In OSN the access to resources and activities between the participants are based on the relationship shared between them [8]. Access control models need to consider that these relationships are not permanent and change over the time. There are three different types of relationships in OSNs: User to User (U2U) relationships, such as Alice friend of Bob; User to Resource relationships (U2R), for example Alice owner of photo01: and, Resource to Resource relationships (R2R), for instance, if Bob posts a comment on Alice's photo, the comment and the photo share a R2R relationship.

F. Relationship Management

It is related with the measure of how specifically a user can establish his relationships. It has been identified three levels of relationship management. The first one is the Fine grained level; this level gives the owner the possibility to create different groups of users; based on these groups, the owner is able to manage the access to his resources. The second level is the Social Circle; it allows the owner to create a social circle of friends in order to grant them access to his resources. In this level, all friends share one access policy; it is not possible to distinguish and create different groups between them. The third level of relationship management is the Shared Secret. In this scheme the shared secret is a proof of the relationship between the owner and the requestor user. The shared secret is distributed between the friends and the owner can manage the access.

Now, let us look at the access control requirements from the point of view of who manages the OSN system. We identify three main features.

1) Resource control

This property defines who decides the access rules in order to grant access to the resources and ensures that users can publish their information without any concern of unauthorized access. There are three approaches: Full Control, Partial Control and No Control. In the Full Control, the owner establishes the rules and decides who can access his resources. In the Partial Control, the owner establishes and decides who can access his resource but the system is responsible for enforcing the rules. In the No Control approach, the system establishes the accessing rules for every user; the owner does not take part on these decisions.

2) Credential distribution

This property is referred to the amount of information that is maintained by the users and the system [9]. There are three types of distribution. The first one, Decentralized; in this distribution there is no a central repository, therefore all the access control credentials are stored in the user side. It requires the cooperation of the resource's owner in order to take an access decision. The second distribution is the Equal Sharing. The system and the user maintain part of the access control; the amount of control depends if it is system oriented or user oriented. The third distribution type is the Centralized. In this distribution all the access control credentials are store in the system.

3) Access control decisions

Access control decisions are referred to who takes decisions in order to grant access to a resource. It is possible to identify local, partial and server based access control decisions. Local, in this type of access control decision it is not needed the interaction of the server because the access decisions are taken at the client side. It is important to notice that the access control decisions are related with the credential distribution. Hence, a local decision needs that all

credentials are stored in the user side. On the other hand, in the Server based, the decisions are made by the server. In the partial approach, the decisions are made either by the server or by the client depending on who stores the access credentials.

Finally, let us look at the access control requirements from the point of view of features offered by the OSN system to the users in order to fulfill certain needs. We identify six requirements.

4) Delegation

Delegation is an important aspect in access control models; it is the process in which a user can empower other users some authorizations in order to carry out specific activities [10]. It has been identified three types of delegations: User Control, N-Model Delegation and System Control. In the User control delegation, the users can delegate access control credentials to other users and depending on the user's policy the users that got the credentials can or cannot delegate them to other users. In the N-Model delegation, the credentials are delegated to the users and they can pass the credentials to other users until it reaches the N level. In the last type of delegation, System control, user cannot delegate the credentials. A user receives the credential, in a one to one correspondence, either by another user or by the system.

5) Transparency

This property is referred to the amount of information about the access control state available to the owner and to the requestor users [11]. There are three levels of transparency: public, partial and system oriented. In the public transparency, the owner and the requestor have all the information available about a specific access control decision. In the partial transparency only the owner or the requestor has the information available about the state of a request but not both. In the system oriented transparency, neither the owner nor the requestor has information about the access control state.

6) Depth

It represents the depth of a relationship. Users normally want to interact with people with relationships close to them such as friends or friends of friends.

7) Trustworthy

Trustworthy is based on the level of trust between two users [8], [12].

8) Data sensitivity

It is referred to the degrees of sensitivity; it allows user to judge the sensitivity level of a resource in order to grant access to it.

9) Conflict resolution policies

Access control models need to provide mechanisms to deal and solve authorization conflicts [13].

We have analyzed some characteristics and requirements that need to be supported by access control solutions for OSN systems; in what follows we are going to study some of the existing and relevant access control models.

III. Existing and Relevant Access Control Models

In this section we present two different schemes; which were selected based on the most recent studies. The selected schemes are: The Social Graph extended Model [2]and the Multiparty Access Control Model[14]. The models were selected based on the analysis of the requirements specified in Section II. We describe each model, its components and its grammar in order to be able to understand and specify the respective access control policies and evaluate the expressiveness of each model through real samples scenarios. After that, we finalize by discussing each model.

A. The Social Graph Model Extended [2]

This model presents an extension applied to the Social Graph Model presented on [15]. The regular expressions used to specify access control policies in [15] are extended in [2] in order to be able to support various types of relationships based access control policies. The model covers U2R and R2R relationships in addition to U2U relationships. The authors consider not only users' normal usage activities but also users' administrative activities. Finally, in order to solve authorization policy conflicts the model includes simple system defined conflict resolution policies.

The model identifies six basic components: users, sessions, resources, policies, social graph and decision module.

Users: A user represents a person who has an account in an OSN system. There two types of users: accessing users, to whom authorization may be granted and the target users, against whom the access is performed.

Sessions: A session is an active instance of a user. Every time that a user logs in an OSN he creates an instance, which is known as session. A session corresponds to a single user. However a user can have multiple sessions and each session can have different access control policies.

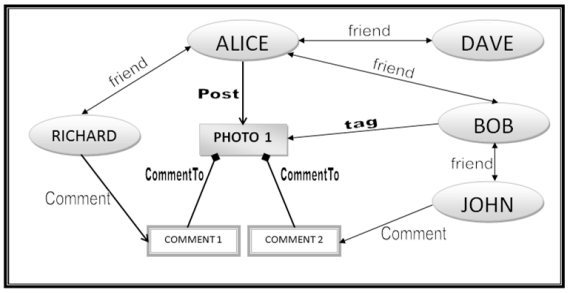

Fig. 2. OSN — Sample social graph extended model.

Resources: A resource is owned by a user that requires to be protected. The user who has the administrative privileges over a resource has to specify the access control policies for it.

Policies: Policies are a set of rules defined by the users or by the system, that handle the access control decisions in order to grant or not authorization for accessing targets.

Social Graph: It represents the relationships between users in an OSN. The model expands the representation presented on [11] by covering not only U2U relationships but also U2R and R2R relationships. Fig. 2 presents a sample Graph Model for an OSN. The Social Graph is defined by three parameters, $G =< V, E, \Sigma >$. As the model incorporates U2R and R2R relationships, V represents a set of users and resources and E is the set of relationships between users and resources and denotes a set of relationship types.

Decision Module: Its work is to consolidate all the policies from users and system in order to make a decision.

B. Policy Specification

First, it is necessary to define the concept of access request. If a user wants to access a target, he needs to specify his request. An access request is defined by three parameters: (s, act, T). Where s indicates the accessing session, act denotes the action that the user wants to perform and T represents the set of targets.

An access control policy specifies the authorized users that can perform a set of actions on a set of targets within an OSN. The model uses the same grammar and policy specification specified on [11]. The social Graph Model represents its policies using regular expressions. The policies are expressed in the following terms (1), (2):

$$Access\ Control\ Policy = Request\ action + Optional\ target\ resource + Required\ Graph\ Rule \quad (1)$$

$$Required\ Graph\ Rule = (start, path\ rule) \quad (2)$$

From (2), $start$ represents the starting node of the evaluation. It could be: u_t; u_c *or* u_a; considering u_a as the accessing user, u_c the controller user and : u_t as the target user and *path rule* is represented by (3) and (4)

$$Path\ rule = collection\ of\ path\ specs \quad (3)$$

$$Path\ specs = (path, hopcount) \quad (4)$$

In (4), *"path"* represents the sequence route involving the relationships between two users and *"hopcount"* indicates the maximum depth in the path, which is represented by the edges on the Social Graph.

As a *"path rule"* is a collection of path specs we need to consider the connectors between them. The model identifies two connectors: conjunction ($\wedge$) and disjunction ($\vee$) and the existence of *wildcards* to represent different occurrence of relationship types. There are three wildcards (5).

$$* \rightarrow 0\ or\ more; \quad + \rightarrow\ 1\ or\ more; \quad ? \rightarrow 0\ or\ 1 \quad (5)$$

Therefore, (6) defines an access control policy.

$$Access\ Control\ Policy \rightarrow < Request\ action, Optional\ target\ resource, (start, path, hopcount) > \quad (6)$$

The optional target *resource* specifies the type of resource. So, this field is used only when the policy is related with a resource; otherwise it is not needed.

The model presented in [2] increments only two notations: Square Brackets and Double Square Brackets. The first one is used to segment a $path\ rule$ that represents a sequence of relationship type expressions. On the other hand, the Double Square Brackets denotes skipping of the path rule contained, which means that the $local\ hopcount$ will not be count in the $global\ hopcount$. Therefore, and Access Control Policy is specified as follows (7):

$$Access\ Control\ Policy \rightarrow < Request\ action, (start, path, hopcount) > \quad (7)$$

C. Conflict Resolution Policies

The authors assume that there are not conflicts with policies specified by the system. However due to policy individualization, multiple access control policies need to be considered in order to make an access decision which could result in decision conflicts. In order to solve these conflicts, the model considers three approaches: disjunctive, conjunctive or prioritized.

In the disjunctive approach, it is enough to satisfy at least one of the policies in order to guarantee access. In the conjunctive approach in order to obtain access it is needed to satisfy all the policies. Finally, the prioritized approach is based on priorities; for instance a parent's policy has more priority that a children's policy.

D. Use Case

We are going to present a police example considering the model's grammar and the OSN's sample presented in Fig. 2.

Example: Dave wants to view Photo 1. Alice posted Photo1 and tagged Bob on it. Dave and Bob are strangers but both are friends of Alice. In (8) we specify the request:

$$(Dave, read, Photo1) \quad (8)$$

where $Dave$ represents the accessing session, $read$ the action to be performed and $Photo\,1$ denotes the target.Second, it is needed to consider the required policies in order to make an access control decision. We have to consider Dave's policy as the accessing user, Alice's policy as the owner of the photo, Bob's policy as the tagged user and System's policy. Dave needs to specify what resources he wants to access. Dave allows himself to access any resource that has a direct relationship with any of his contacts within two hops. His policy is represented in (9):

$$Dave's\ Policy: \langle read, \left(u_a, \left(\left[\sum \rightarrow_{u_u}, 2\right]\left[\left[\sum \rightarrow_{u_r}, 1\right]\right], 2\right)\right)\rangle \quad (9)$$

Dave's contacts within two hops are: Alice (1 hop) and Richard and Bob (2 hops). Consequently, Bob allows himself to read any resource posted by these users. As we can see in the policy above, the $hopcount = 1$ within the double brackets does not count in the final $hopcount = 2$

As Alice is Photo1's controlling user, it is required to consider her policy. Alice allows her friends within 3 hops to access Photo1. (10) is the resultant policy is:

$$Photo1's\ Policy\ by\ Alice: \langle read^{-1}, (t, ([post^{-1}, 1][friend*, 3], 4))\rangle \quad (10)$$

Bob's policy for $Photo1$ has to be considered as well because he is tagged in the photo. Bob is more concern about his privacy so he wants to allow only his direct friends to access this resource. (11) is the corresponding policy is:

$$Photo1's\ Policy\ by\ Bob: \langle read^{-1}, (u_c, ([friend], 1))\rangle \quad (11)$$

On the other hand, the system specifies a policy (9) in which users with any type of relationship within 4 hops can access the related resources.

$$Authorization\ Policy\ by\ System: \langle read, \left(u_a, ([\sum_{u\_u} *, 4][\sum_{u\_r}, 1], 4)\right)\rangle$$

Analysing Bob's Policy and Alice's Policy, it is possible to determine that there is a conflict between these policies. Therefore it is required a Conflict Resolution Policy. As explained above, the conflict resolution policies are specified by the system. The system states that the policies established by the owner override the policies established by the tagged users (10).

$$Conflict\ Resolution\ Policy\ by\ System: \langle read^{-1}, (own > tag)\rangle$$

Finally, having all the required policies it is possible to make an access control decision. Then Dave is allowed to see $Photo1$ because Alice allows him, although Bob does not allow the access.

IV. Discussion

In this section, we present and discuss the strengths and weaknesses of the Social Graph extended Model. First, let us start analyzing the strengths of the Social Graph model.

- The model considers users and resources as targets. This is an important characteristic, because in OSNs many activities are performed against users. Therefore, it is important to protect the privacy from resources as well as users.
- The model allows not only to the resource owner but also users related with the resource, such as a tagged users, to specify the corresponding access control policies according to their needs.
- Access conditions are based on a maximum depth level and the model also allows to deny relationships types. For instance, if a user wants to allow access to a document *file1,* to his friends, friends of his coworkers or coworkers of his coworkers but not to his direct coworkers, he can specify the following path:

$(f * c *\wedge \neg c,\ 2)$. Although, the depth of the path is 2, the negative authorization permits to deny the access to specific relationships with a deep of 1.

- In OSN systems, there are three types of relationships, U2U, U2R and R2R relationships. The model considers these three scenarios and allows users to specify the policies based on these relationships. In fact, the model treats resources and users as nodes and the actions that users perform against the resources are identified as relationships. For instance, Alice can specify a policy to regulate that only users, who have posted comments on the same photos as she commented on, can poke her.
- The Social Graph Model allows the combination of different relationship types such as friend of, coworker of, child of, parent of.
- The model proposes a simple solution through administrative policies for collaborative access control. It incorporates a Decision Module and conflict resolutions policies; which are specified completely by the system.
- Now, let us analyze the weaknesses of the model, considering the features that the model try to fulfill but it does not satisfy well and the requirements that are not considered by the Social Graph Model.
- Although, the model considers negative authorization, it is necessary to explicitly specify which relationships are not allowed, which could turn out to be tedious and time consuming.For example, if a user only wants to grant access to his indirect friends with a $depth = 5$; he should establish the following path: $(f *\wedge \neg f \wedge \neg ff \wedge \neg fff \wedge \neg ffff,\ 5)$ indicating all the depth relationships that are not allowed.Thus, in order to grant access to users at distance N without granting it to those a distance N-1 it is required to specify all the denied paths.
- Furthermore, the negation symbol ¬ considered for the negative authorization can be used only with relationship paths but not with specific nodes. Therefore, if Alice wants to grant access to her photo to all her friends except Dave, the model does not allow her to establish this access control policy.
- Even though, not only the owner of a resource but also the users related with the resource can specify the corresponding policies, the mechanisms that the System uses to resolve possible conflicts are not well considered. The model proposes three mechanisms, disjunctive, conjunctive or prioritized but it is not explained the assumptions, considerations and parameters that system will use to select the approach.
- Now, if we consider that the system selects a prioritized approach, and the policies of the owner overrides the policies of the users related with the resources; the model does not consider the possibility that one resource could have more than one owner. For example, if Bob and Alice are owners of the document *file1,* Bob establishes that his friends with a depth of 3 can access *file1* and Alice specifies that her friends with a depth of 1 can access it. As we can see, these two different policies have raised a conflict problem. It is not possible to determine which policy or how the policies are going to be combined to make an access control decision.
- It is not possible to specify access to a resource based on information of the users, such as name or location. For example, Alice wants to allow access to her document *file1* only to Bob. The grammar specified by the model does not allow users to state this type of policies.
- The model does not consider the following requirements: delegation, trustworthy and data sensitive levels.

A. Multiparty Access Control [14]

The Multiparty Access Control Model (MPAC) presents a solution to facilitate collaborative management of shared data in OSNs and captures the core features of multiparty authorization requirements. To make a final access control decision, the model checks the access request and the policies established by each controller. As data controllers may produce different decisions for an access request, conflicts may occur. Therefore the model also introduces a voting scheme for resolving multiparty privacy conflicts.

Before proceeding to identify the main components of MPAC Model, let us consider the following scenario to explain each of them: Alice is an OSN user. She decides to upload a photo on her space and tags Dave on the photo. Then, Dave decides to share Alice's photo with his friend and posts it on his space. On the other hand, John publishes some information on Dave's space.

The main components identified are:

- *Controllers:* As mentioned before, the model considers a

multiuser environment. Hence, it considers multiple controllers to specify access control policies over the shared data. A controller is a user of the OSN who is related with the data and can regulate its access [16]. There are four types of controllers.

Owner: is a user who has a space. All data on his space is owned by him. In the previous scenario, Alice is the owner of the photo.

Contributor: if a user publishes some data in other user's space, he is considered the contributor of the data. In our sample scenario, John is the contributor and Dave is the owner.

Stakeholder: is a user who has been tagged on a data item that is published on someone else's space. For example, because Dave is tagged on Alice's photo, he is a stakeholder.

Disseminator: when a user share some data from someone else's space and publishes the data on his profile, the user is considered the disseminator of the data. For instance, when Dave decides to share Alice's photo, he is the disseminator of the data.

- *Relationship Type:* represents a set of relationships supported the OSN system. For example: $friend\ Of$, $colleage\ Of$.
- *Group:* represents a set of users, who usually shares the same interests for example a *Fashion Group*
- *Accessor Specification:* the set of users who are granted to access the shared data are considered accessors. An accessor can be represented by a user, a relationship type or a group.
- *Data Specification:* each user has data, which is composed of three types of information: user profile, user relationship and user content. A profile is a space where a user can upload photos, documents, personal information and more. The relationships represent the set of relationships established by the owner with other users. The content indicates the information and resources that the owner has decided to publish on his profile.

MPAC model represents an OSN system with a labeled graph, which consists of three main parts: a relationship network, a set of user groups and a collection of user data.

B. Policy Specification

The policy specification is based on the components identified in the model. In Table I, we represent the components, explained in the previous section, with its formal definitions and notations in order to facilitate the understanding of MPAC Policy.

The multiparty access control policy is defined as follows (11):

$$P = \langle controller, ctype, \{\langle ac, at\rangle\}, \langle dt, sl\rangle, effect\rangle \quad (11)$$

where:

$controller$ is a user who can regulate the access to the data

$ctype$is the controller type

$effect$, it represents the authorization result of the policy, can take two values: permit or deny.

1) Use case

We are going to present a police example considering the model's grammar and the OSN. We identify the sensitive levels between$[0,1]$, where (0.00) indicates none sensitive level and (1.00) represents the highest sensitive level.

Example: Alice uploads a photo *photo01* with a sensitive level of 0.5 on her profile and she wants to allow all her friends to access it. The corresponding policy is (12):

$$Photo's\ policy\ by\ Alice: \quad (12)$$
$$(Alice, OW, \{\langle friendOf, RN\rangle\}, \langle photo01, 0.50\rangle, permit\ )$$

As Alice tagged Bob in the photo, he also wants to specify the access to it (13); and he decides that only the members of the soccer group are allowed to see the photo. Moreover, he states that the *photo01*'s sensitive level is 0.75

$$Photo's\ policy\ by\ Bob: \quad (13)$$
$$(Bob, ST, \{\langle Soccer, GN\rangle\}, \langle photo01, 0.75\rangle, permit)$$

2) Conflict resolution and policy evaluation

In order to evaluate and access request considering multiparty access control policies, the model analyses the access request and checks it against the policy specified by each controller. Then, the evaluation process returns a decision allowing or denying the access. The number of individual decisions depends on the number of controllers. Therefore, in order to have a final decision for the access request, all the individual decisions are aggregated. Due to we have different individual decisions, depending on the number of controllers, and each controller has different privacy concerns, conflicts may occur.

TABLE I: MULTIPARTY MODEL'S COMPONENTS

Component		Formal Definition	
Type of Controller	Owner	ct	OW
	Contributor		CB
	Stakeholder		ST
	Disseminator		DS
Accessor Specification		ac	
Type of Accessor Specification	User Name	at	UN
	Relationship type		RT
	Group Name		GN
Data Specification	Data item	D	dt
	Sensitive level		$sl; rational\ num\ between\ [0,1]$

Let us consider the example above, Alice and Bob are the controllers of the photo. Alice specifies that only her friends can access it but Bob states that only members of the Soccer Group can access it. Hence, we have conflicts on the final decision and the model needs to provide mechanisms to solve those conflicts during the policy evaluation process.

In order to resolve these conflicts with multiparty policies, MPAC model proposes a voting scheme.

C. Voting Scheme

The voting scheme proposed by the model to resolve multiparty conflicts, consists of two voting mechanisms, decision voting and sensitive voting. The model considers the aggregated decision value and the sensitive score to propose a threshold-based conflict resolution. Where, the decision is $permit$ if the aggregated decision value is greater than the sensitive score; otherwise, the decision result is $deny$.

D. Strategy-Based Conflict Resolution

In real OSN scenarios, many controllers may have different priorities, which will impact on the final decision. The model assigns the most important priority to the owner of the data. The mechanisms proposed by the model are: owner overrides, full-consensus-permit and majority-permit. These mechanisms could be used as guidelines for the owner of the data.

1) Discussion

In this section, we present and discuss the strengths and weaknesses of the Multiparty Access Control Model. First, let us start analyzing the strengths presented in the MPAC model.

- Although, the model does not permit to explicitly specify the depth of a relationship, such as $depth = 4$; it considers different relationship types that can satisfy this requirement, such as friend of, colleague of or friend of friend(FOF). For instance, if Alice wants to grant access to her photo to her friends with $depth = 4$, she needs to specify($FOFOFOF$).
- The model considers the existence of groups in OSNS and allows users to specify access control policies to allow members of the groups to access their resources. For example, Bob can grant access to his photos only to members of the soccer group.
- The model considers different type of controllers. Not only the owner can specify access control policies but also contributors, stakeholders and disseminators.
- The grammar used to specify the access control policies allows or denies access to users by their names, relationship type or group members. For example, Bob can state an access control policy to permit Alice to access to her photo.
- The model considers the sensitive level of the data. In fact, this parameter is used to solve conflict resolution problems.
- In order to solve conflict resolution problems presented by multiparty access control policies, the model proposes a voting scheme. It considers the aggregated decision value and the sensitive score. Although, these parameters are not related with each other, it is possible to use them to solve conflict problems by intuitively assuming that a lower level of sensitive score requires lower level of agreement and higher level of sensitive score requires a higher aggregated decision value.

Second, let us analyze the weaknesses of the model, considering the features that the model try to fulfill but it does not satisfy well and the requirements that are not considered by the MPAC model.

- MPAC model only considers U2R relationships. However, in OSNs it is possible to find U2U and R2R relationships.
- The grammar of the model does not consider users as a target. For instance, if Alice wants to specify who can poke her, the model cannot symbolize this access control policy.
- The MPAC model does not allow us to specify different activities that users can perform in OSNs. The unique action considered by MPAC is to permit or deny the access. Hence, if Alice, the owner of *file1*, wants to assign read permission to Bob and write permission to Dave over *file1;* she cannot express these policies with the grammar specified by the model.
- Although, the model considers certain type of relationship's depth, it only considers the maximum depth level to specify access control policies. It is not possible to grant access to user with a depth distance of N without granting it to users with a distance N-1. For example, if Alice wants to grant access to her photo to her indirect friends with a $depth = 4$, the model does not allow to state this policy.
- Even though, the model allows users to use the name of their friends to establish access control policies to permit or deny access, it does not allow them to consider other type of information such as location. For example, a user cannot grant access to his photo only to his friends that live in Sydney.
- MPAC proposes a weighted decision, but it is not explain how the weights are assigned, which parameters are used and who decides the corresponding weights for each controller.
- If we analyze the sensitive score, it is possible that one user believes that the data is high sensitive and assigns the maximum value to the data but the rest of controllers believe that the data is not sensitive and assign a low level of sensitivity. Because, the sensitive level is calculated using (14), the final sensitive score will be low and therefore, the aggregated decision value required to permit the access will be lower too.

$$SC = \left(SL_{ow} + SL_{cb} + \sum_{i \epsilon SS} SL_{st}^{i}\right) \times \frac{1}{m} \quad (14)$$

- The model also provides a strategy based conflict resolution mechanism, which give to the owner three different approaches to resolve conflict problems; owner-overrides, full-consensus permit and majority-permit. If the owner chooses an owner-overrides approach, the policies established by the rest of controllers will not be take into account. For instance, as a stakeholder, contributor or disseminator it does not have sense to establish the access control policies if at the end the owner decides to ignore them.
- MPAC model does not consider conflict intersection problems between policies established by the same users. For example, Bob establishes one policy and to allow access to his photo to all the member of the Soccer group. Then, he also states that none of his friends can access it. Fred is member of the soccer group, so he can access the photo according to the first policy. But Fred is also Bob's friend; hence, according to the second policy he cannot access it. MPAC does not provide mechanisms to solve this type of conflicts.

V. Comparative Analysis of Models

In this section, we present a comparative analysis of the Social Graph Model and the Multiparty Access Control Model based on the access control requirements established on Section II.

As we can see on Table II, the requirements form the rows of the table and the models are evaluated based on their characteristics in order to determine the properties of the

models and whether they fulfill or not these needs.

TABLE II: COMPARATIVE ANALYSIS OF THE SOCIAL GRAPH MODEL AND THE MPAC MODEL

Requirements	Social Graph Model	MPAC Model
Access control requirements from the point of view of the user and the source that is going to be accessed		
Requestor identity	Listing	Listing
Mapping authority	Owner	Owner
User and Resource as a Target	Yes	No The model considers only Resources as targets.
Police Individualization	Yes	Yes
Relationship-based U2U, U2R, R2R	Yes	No The model only considers U2U and U2R
Relationship management	Social Circle	Fine grained level
Access control requirements from the point of view of who manages the OSN system		
Resource control	Full Control	Full Control
Credential distribution	Equal sharing	Decentralized
Access controldecisions	Local	Local
Access control requirements from the point of view of features offered by the OSN system to the users in order to fulfil certain needs		
Delegation	No, System Control	No, System Control
Transparency	Partial, Only target users know which user has access to their resources.	Partial, Controllers know how can or cannot access to their resources.
Depth	Yes	Yes
Trustworthy	No	No
Data sensitivity	No	Yes
Conflict resolution Policies	Yes, The model considers Conflict resolution policies specified by the system.	Yes, As a conflict resolution strategy, MPAC model introduces a voting scheme.

VI. CONCLUSIONS AND FUTURE WORK

In this section we discuss the possible improvements and future directions that can help to capture new access control requirements that are presented in the dynamic developments of social networks; which also may address to model more expressive access control policies. The outcomes may constitute a basis for further study or research.

As part of the results in this work, we have identified some weaknesses in current access control models that need to be exploited in order to provide users more flexible mechanism to control their own information and resources on Online Social Networks. We consider that some of the weaknesses found in the analyzed schemes can be solved by changing or adding few parameters that can increase the expressiveness of the models. For instance, let us consider the social graph model, in this scheme the access control policies are specified as (15):

$$Access\ Control\ Policy \rightarrow \\ < Request\ action, (start, path, hopcount) > \quad (15)$$

One of the softness of the model is the depth problem; in which, to grant access to users at distance N without granting it to those a distance N-1 it is required to specify all the denied paths, which could become tedious and time consuming. It is possible to solve this problem by replacing the meaning of $hopcount$. In the actual model, $hopcount$ represents the maximum depth in the path. However, we could consider $hopcount$ as a set of depth relationships. Therefore, if a user only wants to grant access to his indirect friends with a $depth = 5\ or\ 6$; instead of establishing the following path $(f* \wedge \neg f \wedge \neg ff \wedge \neg fff \wedge \neg ffff,\ 6)$, he could establish$(f*, \{5,\ 6\})$; where $\{5,6\}$ represents the valid depth of the relationships.

To mention another example, in the access control policy established by the social graph model, it is possible to add one parameter to represent the sensitive level of data specification, similar to the one considered in the MPAC model.

In fact, each scheme studied presents different strengths that the other one does not contemplate. One of the main fortes of the social graph model is that it considers the three types of relationships existing in OSNs, U2U, U2R and R2R relationships. On the other hand, MPAC model introduces sensitive levels for data specification and considers different types of users in OSNs. Therefore, as part of future work we are planning to propose a new access control model using as basis the combination and the strengths of these two schemes.

Due to the dynamic and quick evolution of OSNs more activities and information of users are available in these systems. Then, in order to capture these fast developments and new features, access control models need to incorporate new mechanisms. We would further investigate some solutions such as to incorporate some predicate expressions for attribute based control and to use the public information available in OSNs systems [17] in our future work. As an example, with the increase of the GPS enable devices, one of the characteristics that can be considered is to capture the users' geographical location information at the moment that they initialize a session in the system, in order to define distinct access control policies; which could allow access control models to satisfy different users' requirements such as, if Alice is at her work she does not want to be contacted by her friends.

Last but not least future direction is to investigate mechanisms to solve conflict policies that can be raised in multiparty environments. One direction would be to consider adding a function called $reputation\ (Rp)$. The function can be represented as follows $Rp(A, B) = z$; where the outcome of the function is a number and the function represents a U2U relationship. Then, it is possible to order these reputations between users in order to solve conflicts on policy schemes. If $Rp(C, A) > Rp(C, B)$ then the policies of A have higher priority than the policies established by B.

In this section we have planned and analyzed to extend our work in several directions in order to improve the expressiveness of actual access control models and provide users better mechanisms to satisfy their needs in this changing environment of Online Social Networks.

As result of this analysis, it is important to mention that it is necessary to improve the expressiveness of actual access control models and provide users better mechanisms to satisfy their needs.

REFERENCES

[1] A. Ahmad and B. Whitworth, "Access control taxonomy for social networks," in *Proc. 7th International Conference on Information Assurance and Security (IAS)*, 2011, pp. 256-261.

[2] Y. Cheng, P. Jaehong, and R. Sandhu, "Relationship-based access control for online social networks: Beyond user-to-user relationships," in *Proc. International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, 2012, pp. 646-655.

[3] M. Madejski, M. Johnson, and S. Bellovin, "The failure of online social network privacy settings," 2011.

[4] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: Automated identity theft attacks on social networks," in *Proc. the 18th International Conference on World Wide Web*, 2009.

[5] H. Hu and G.-J. Ahn, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," presented at the 27th Annual Computer Security Applications Conference, ACSAC'11, 2011.

[6] K. Thomas, C. Grier, and D. Nicol, "Unfriendly: Multi-party privacy risks in social networks," presented at the 10th International Conference on Privacy Enhancing Technologies, Springer-Verlag, 2010.

[7] A. Masoumzadeh and J. Joshi, "Osnac: An ontology-based acccess control for social computing," presented at IEEE Social Computing, (SocialCom), 2010.

[8] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 1, pp. 6:1-6:38, 2009.

[9] K. Kane and J. Browne, "On classifying access control implementations for distributed systems," presented at the Eleventh ACM Symposium on Access Control Models and Technologies, ACM, Lake Tahoe, California, 2006.

[10] M. Ben-Ghorbel, F. Cuppens, N. Cuppens-Boulahia, and A. Bouhoula, "Managing delegation in access control models," presented at 15th International Conference on Advanced Computing and Communications, ADCOM, 2007.

[11] R. Oliver, *What Is Transparency*? New York: Mc-Graw Hill, 2004.

[12] Y. Sun, C. Zhang, J. Pang, B. Alcalde, and S. Mauw, "A trust-augmented voting scheme for collavorative privacy management," *Journal of Computer Security*, vol. 20, no. 4, pp. 437-459, 2012.

[13] P. Fong and I. Siahaan, "Relationship-Based access control policies and their policy languages," presented at the 16th ACM Symposium on Access Control Models and Technologies, SACMAT, New York, 2011.

[14] H. Hogxin, G.-J. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: Model and mechanisms," *IEEE Transactions on Knowledge and Data Engineering*, 2012.

[15] Y. Cheng, J. Park, and R. Sandhu, "A user-to-user relationship-based accesss control Model for online social networks," presented at the 26th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy, France, 2012.

[16] H. Hu and G.-J. Ahn, "Multiparty authorization framework for data sharing in online social networks," presented at the 25th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy, Berlin, 2012.

[17] J. Pang and Y. Zhan, "A new access control scheme for Facebook-style social networks," no. 1304.2504, 2013.

Gabriela Suntaxi-Oña is current a lecturer at National Polytechnic School. In 2010, she graduated in computer systems engineering and computing at the National Polytechnic School. She did her graduate studies at Macquarie University, Australia, sponsored by a SENESCYT scholarship. In 2013, she obtained her master's degree in information technology in systems security. In August 2015, she is going to start working as an assistant researcher and begin her doctoral studies at Karlsruhe Institute of Technology, Germany. Her research interests include computer security, access control models and data encryption in the cloud.

Vijay Varadharajan is currently a professor and the Microsoft chair in innovation in computing at Macquarie University (2001-todate). He is also the the director of Advanced Cyber Security Research Centre (ACSRC). Before this he was the dean of School of Computing and IT at University of Western Sydney (1996-2000).

Previously, Vijay has headed security research at HP Labs Bristol, UK (1988-1995). During his tenure at HP Labs., under his leadership, some 6 different security technologies were transferred into successful HP products in divisions. He also headed the technical security strategy initiative at HP under the senior vice president. Before this, he was a research manager at British Telecom Research Labs. U.K (1987-88). From 1985 till 1987, he was a research fellow and a lecturer in computer science at Plymouth and Reading Universities. He did his Ph.D in computer and communication security in the U.K (1981-1984) from Plymouth and Exeter Universities in U.K., which was sponsored by BT Research Labs. He did his electronic engineering degree from Sussex University, UK (1978-1981). He was awarded the 1981 Prize of the Institution of Electrical Engineers, IEE, for outstanding performance at Sussex University and the Committee of Vice Chancellors and Principals Award (UK).