ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.11

An Online Social Networks for Access Control Model Using User-To-User Relationships

Sreenu Banoth[1], Biyyala Prashanth[2]
Assistant Professor[1, 2]
Department of CSE
WITS, Warangal, India

Abstract:
Users and resources in online social networks (OSNs) are interconnected via various types of relationships. In particular, user-to-user relationships form the basis of the OSN structure, and play a significant role in specifying and enforcing access control. Individual users and the OSN provider should be enabled to specify which access can be granted in terms of existing relationships. In this paper, we propose a novel user-to-user relationship-based access control (UURAC) model for OSN systems that utilizes regular expression notation for such policy specification. Access control policies on users and resources are composed in terms of requested action, multiple relationship types, the starting point of the evaluation, and the number of hops on the path. We present two path checking algorithms to determine whether the required relationship path between users for a given access request exists. We validate the feasibility of our approach by implementing a prototype system and evaluating the performance of these two algorithms.

Keywords: Social network, access control, security model, policy specification.

1. INTRODUCTION

Online social networks (OSNs) are social networks that are established through web-based services through which people can foster social relationships. Sites such as LinkedIn, Facebook, Google+, MySpace, etc, are therefore type of OSNs (Hafez Ninggal, Abawajy, 2011), but also blogging services, peer-to-peer, collaborative and content sharing sites such as Youtube and Flicker, and social bookmarking services such as CiteULike are also types of OSNs. Users of OSNs create their own social spaces and upload different types of personal data such as photos, videos, texts, etc. OSNs facilitate easy social interaction by allowing users to establish relationships and connect to other users, who may be friends in the offline world or strangers. One of the fundamental features of OSNs is the ability to share personal data with others in a relatively privacy-preserving manner. The recent surge of interest in OSNs has been coupled with serious privacy and security concerns, primarily caused by the lack of proper data protection means (Cutillo, Molva, & Strufe, 2009). For instance, users' privacy concerns have affected the popularity of MySpace. Studies have showed that due to lack of privacy control on MySpace, users have abandoned this OSN (Baracaldo, López, Anwar, & Lewis, 2011) and have migrated to other OSNs for their better privacy-preserving means. Access control mechanisms are employed in OSNs to enable users to control the dissemination of their own data and protect their privacy accordingly (Abiteboul et al., 2005). Other approaches are employed to protect rights and ownership of data, such as digital rights management (Rodriguez, Rodriguez, Carreras, & Delgado 2009), which we will review later, and watermarking of individual data (Bedi, Wadhai, Sugandhi, & Mirajkar, 2005). Both these approaches and access control models are intended to improve privacy preservation of OSN users. However, there are many underlying problems in access control mechanisms used in current OSNs. First, only a small percentage of users change the default access control settings to define their own access control policies (Gross & Acquisti, 2005). Second, when these access control mechanisms are used they fail to address the required fine-grained control to avoid privacy violations (Masoumzadeh & Joshi, 2010). The sensitive personal data in OSNs requires a highlevel of protection by means of appropriate access control (Gates, 2007). An inherent challenge is how to define an appropriate ACM to regulate access to OSNs' users' data. ACMs should offer a fine-grained control that captures the specific structure and features of an OSN. Mostly, data dissemination is based on relationships represented in the OSN. Therefore, simple access control lists (Cankaya, 2011) and even more advanced classical ACMs fail to satisfy access control requirements of OSN, as they are not based on the specific properties of social relationships. Recently, various ACMs have been specifically proposed to address OSN privacy-protection requirements. In this chapter we focus on OSN-specific problems and requirements and how those are tackled by different ACMs.

2. BACKGROUND AND PRELIMINARY NOTION

2.1 Online Social Networks

A social network (SN) is a set of people connected to each other by social relationships. Offline Social Networks refer to real-world social communities. Online Social Networks (OSNs) are web based services that offer the functionality of creating a personal representation of one's self through which one can socialize with others. A user is represented in the OSN via a profile to which personal data can be added. An owner is a user who adds her data, referred to as objects, and can share them with others. A main feature of OSNs is the articulation of various types of relationships between profiles to facilitate the social communication with others. The social communication includes various activities such as sharing objects, creating groups, organizing online and offline events, etc. Users in an OSN and their relationships form a social graph. Nodes and

links in the graph denote users and relationships, respectively (Carminati, Ferrari, & Perego, 2006b). Each pair of users in the graph is connected via a path of links between them. The distance between two users measures the number of links of the shortest path between the two corresponding nodes. The social graph is commonly utilized as an abstraction of OSNs upon which ACMs are formalized.

2.2 Access Control Models

An access control model (ACM) is a formalization of how policies are composed based on a specific set of features in the system to regulate and authorise access to data. An access control policy defines constraints on whether an access request to an object should be granted or denied. In the context of OSNs, a request or initiates a request asking for a specific permission on a specific object from its owner. The owner regulates access to and dissemination of her objects by means of defined access control policies. Once a request is authorised, the specific set of permissions entailed by the policy will be granted to the requestor, who is then referred to as the accessor. Delegation is entrusting a user (delegate) to act on an object with the authority of the object owner (delegator). Delegation of authority is convenient for OSNs where users trust each other to further disseminate their objects over the network. Access control is a two-fold control, authoritative or prohibitive. Most ACMs formalize authoritative, or positive, policies only by assuming a closed-world model (Samarati & Vimercati, 2001). In the closed-world model a request can only be honored by an existing authoritative policy or else it will be denied. In many cases, conflicting policies and hierarchy-propagated policies (Carminati, Ferrari, Heatherly, Kantarcioglu, & Thuraisingham, 2009) might unexpectedly authorise a request and violate the privacy of the owner. Therefore, prohibitive, or negative, policies are crucial to limit accidental authorisations of positive policies. Positive and negative policies are enforced in access control in a mutual exclusion pattern (Samarati & Vimercati, 2001). This pattern authorises a request if this request is entailed by a positive policy and not denied by a negative policy. This approach ensures more controlled authorisation, contributing to more protection against imprecisely defined access control policies.

For each ACM there should be a specific enforcement mechanism to enforce policies in the system. The enforcement mechanism verifies a request and matches it against defined policies to infer an authorisation decision with the right permission to be granted. In OSNs, either a centralized authority, a reference monitor, decentralized authorities or users themselves, can carry out policies enforcement. Next, we will review the central classical ACMs to establish a sufficient background, before discussing OSN-specific models.

2.3 Classical Access Control Models

Access control mechanisms are used in information systems to mitigate security and privacy risks of unauthorised access to data. Those mechanisms vary depending on the underlying structure of the system and the levels of protection needed. The first abstraction of an access control model is the access control matrix (Lampson, 1974). The matrix model describes the system as a protection state by defining a list of access permissions of each subject. A reference monitor guards access to objects based on the protection state of the system. A major drawback of this model is the static nature of defining permissions for all the system's subjects. The matrix model lacks abstraction possibilities for groups of subjects and objects. This entails that for each new subject in the system, new lists should be created to guard access to each existing object; the same also applies for each new object in the system. The overhead of changing the protection state limits the applicability of the matrix in large-scale systems. More advanced models expand upon earlier models with specific enhancements to address requirements, identified weaknesses and limitations in expressiveness. These models are more suited to emerging structure and context changes of systems.

2.4 Administrative Access Control Models

ACMs can be categorized into three models based on the administration method (Chinaei, Barker, Frank &, 2009):

1. Mandatory Access Control (MAC) (Bell & LaPadula, 1973) is a central authority system that enforces a lattice-based representation of objects and subjects using specific security or sensitivity levels. System administrators define the security level classifications of subjects and objects to guard access authorisations in the system. A policy constrains access based on the security level of the requestor and the security level of the object to be accessed. MAC models are employed in systems where high security needs to be maintained. 2. Discretionary Access Control (DAC) (United States Department of Defense, 1985), or identity-based access control (IBAC), enables system subjects to decide on how to grant permissions to other subjects in the system without any authority involvement. A subject is entitled to define constraints that should be satisfied by an entity in order to be granted specific access permission. DAC models are employed in systems where subjects are responsible for guarding access to their own objects, e.g., OSNs. Other models such as the model of Carminati, Ferrari, Heatherly, Kantarcioglu, and Thuraisingham (2009) extend the DAC concept by enabling users to also define sets of constraints to filter access requests before granting access. DAC and MAC are not mutually exclusive and can be jointly applied, as in the Chinese Wall model (Kessler, 1992). 3. Role-based Access Control (RBAC) is an alternative model for systems that define specific roles of subjects. Roles are abstract descriptions of what subjects are entitled to perform in the system. Access to an object is dependent on the role assigned to the requestor and the permissions associated to this role. Roles can have different positive and negative permissions, if the model defines negative policies. When different roles are assigned to one subject then the authorised permissions might result in conflicts. The main issues of concern in RBAC are how to assign roles to subjects statically and/or dynamically, and how to guarantee that no conflicts will arise. $f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos\frac{n\pi x}{L} + b_n \sin\frac{n\pi x}{L} \right)$. Chen and Sandhu (1995) addressed the assignment of non-conflicting roles by applying constraints.In their approach, constraints can be used as invariants in the system or preconditions for an action. For example, mutually exclusive roles can be validated by constraints to check that a user cannot have the two roles assigned at once (F. Chen & Sandhu, 1995). Schaad (2001) argues that the Separation of Duty constraints proposed by F. Chen and Sandhu (1995) could still cause conflicts if users are able to delegate roles. Schaad (2001) proposed a rule-based declarative separation of duty approach to statically and dynamically detect role-assignment constraint conflicts and further prohibit delegation of roles. In principal, separation of roles can be guaranteed (H. Chen & Li, 2006) based on the requirements highlighted in the work of Clark and Wilson (1987).

2.5 Attribute---based Access Control Models

Attribute-based Access control (ABAC) is another kind of access control model. ABAC formally describes policies based

on attributes of subjects, objects and other environment-specific data. In comparison with RBAC, ABAC is more flexible by facilitating the definition of rich and finegrained policies. Attribute based encryption (ABE) is a more secure version of ABAC. In ABE, attributes are encrypted using a public and a secret key and distributed to users to which the composition of attributes applies. Bethencourt, Sahai, and Waters (2007) employ ABE for a group-based access control. In their Ciphertext-Policy Attribute-based Encryption model, private keys are defined by a set of attributes and embodied in the form of ciphertext. The ciphertext is a two-part component: an encrypted object and a set of attributes involved in the access control policy. For a request to be authorised, the attributes of the requestor must comply with the ciphertext's attribute component. The policies can be expressed in a collision-resistant monotonic access tree structure. This structure allows a user to have access to more than one private key without being able to aggregate the keys or attributes to access data. Classic policy models are not targeted to a specific type of system. In general, those models are too abstract to be employed in collaborative systems such as OSNs. OSNs systems have a particular structure and type of communication that requires flexible and highly expressive ACMs. Classical models fail to fully address the requirements of OSNs. However, we will discuss later in this chapter some classical models that have been adapted to OSNs. The adaptations basically focus on exerting more dynamic policy definition mechanisms using specific OSN features to support high granularity protection (Tolone, Ahn, Pai, & Hong, 2005).

3. ACCESS CONTROL IN ONLINE SOCIAL NETWORKS

In this section we provide an extensive overview of the main aspects of access control models as solutions to various privacy-related issues in OSNs. We start off by reviewing the main privacy problems reported in OSNs. We then provide the essential requirements proposed for OSN specific ACMs. Then we survey the most prominent OSN-tailored ACMs. In the description of each model, we highlight the main contribution of the model and different approaches. Towards the end of the chapter, we discuss the points in which ACMs need to be enhanced to address open privacy issues. We conclude our discussion by proposing more extensive requirements to fulfill the discussed issues of current OSN-specific ACMs, and to be considered in future research in this domain.

3.1 Privacy Risks in Online Social Networks

OSNs have grown in popularity and become a worldwide phenomenon (A. C. Squicciarini & Sundareswaran, 2009). The main features of fostering relationships and sharing data OSNs attract up to 4 users among each 5 Internet users (The State of Social Media 2011: Social is the new normal, 2012). Nonetheless, those features involve many privacy risks. A risk is defined as the insecurity about a potential negative consequence of a specific action (Havlena & DeSarbo, 1991) that is proportional to the likelihood of the negative consequence (Peter & Tarpey, 1975). Estimating risks is strongly coupled with how users perceive their privacy (Norberg, Horne, & Horne, 2007). The indisputable problem in OSNs is that users fail to correctly estimate privacy risks (Acquisti and Grossklags, 2005) and fail to match them to their actual behaviours in the OSNs (Spiekermann, Grossklags, & Berendt, 2001); this is due to many reasons as we will discuss here. Acquisti and Grossklags (2005) highlight the following reasons that hinder making proper privacy decisions:

- *Incomplete information* about the possible accessors that makes the risks involved indeterministic especially for external parties accessors. - *Bounded rationality* (Simon, 1982) limits user's ability to rationalize about all available data. Even if a user has access to all data about possible accessors and who should not have access due to all the possible risks, the user's mental model would simplify the quantitative facts when making privacy-related decisions. The inferred decisions might be not very accurate for defining certain policies. - Social preferences and patterns of data disclosure affect users' decisions. Complete information utilization would not prevent privacy-related decisions from deviating from rationality under those effects. - Failure in predicting the future preferences and the tendency to compromise in the present to get immediate benefits affects the future privacy status of users. Users lack proper information about how to make informed privacy decisions (Acquisti & Grossklags, 2005). Therefore, the outcome of the decisions they make using the privacy management tools in current OSNs clashes with their expectations. In Facebook, only about 40% of the privacy settings enable access to data as the owner expects (Lipford, Besmer, & Watson, 2008). The rest of the settings enable more users to access than the owner expects. Users contribute to this discrepancy by acting differently to the privacy concerns they express. Norberg, Horne and Horne (2007) coined the term "privacy paradox" to describe the relationship between users' intentions of disclosure and their actual behaviour. When users grant access to their data, they are concerned about their privacy. However, these concerns are multi-faceted. Users are more concerned about privacy when disclosing to close friends than to strangers (Gross & Acquisti, 2005). This can be explained based on the incomplete information factor about weak ties shared with strangers (Granovetter, 1973). OSNs facilitate the fostering and managing of a large number of weak ties very easily. Reasoning about the incomplete information to estimate privacy risks of weak ties makes those ties one the main reasons behind the difficulty of managing privacy in OSNs (Donath & Boyd, 2004). In addition, trust plays a significant role in disclosure decisions (Norberg, Horne, & Horne, 2007). Estimating trust for weak ties is a challenge that results in privacy risks. The patterns of data sharing in OSNs further complicate reasoning about privacy. OSN users aim at expanding their social interactions within the network and sharing their objects on a large scale (A. C. Squicciarini, Shehab, & Wede, 2010). Indeed, OSNs are designed to encourage users to share. For instance, Facebook is designed to encourage disclosure of as much information as possible (Hu, Gail-Joon, & Jan, 2012). Facebook status textbox encourages users to update the status by showing the text "What's on your mind?" in order to encourage users to write what's on their minds as their status. Facebook users reveal significantly more identifying information about themselves than users in other OSNs (Dwyer, Hiltz, & Passerini, 2007), (Gross and Acquisti, 2005). A personal information revelation study states "Participants are happy to disclose as much information as possible to as many people as possible" (Gross and Acquisti, 2005, p. 2). As the social interactions evolve, more privacy threats arise. Social interactions with friends and friends of friends and so on, might lead to inappropriate disclosure of private information. This is often the case when users are not aware of who can access their objects (A. C. Squicciarini, Shehab, & Wede, 2010; Hogben, 2008). Trying to mitigate privacy risks by limiting interaction on OSNs would not satisfy user's needs. ACMs employed in OSNs should facilitate maximal privacy-preservation without hindering interaction. Access control tools in current OSNs are

generally simplistic and coarse-grained (A. C. Squicciarini, Shehab, & Wede, 2010; Masoumzadeh & Joshi, 2010), which occasionally contributes to the failure of privacy protection required by users. All the reasons mentioned above contribute to specifically making OSNs users the victims of privacy violations (H. Wang & Sun, 2010). We will now list the main OSNs challenges and privacy risks reported in the literature: - Automatic identity theft (Leyla, Thorsten, Davide, & Engin, 2009), where an attacker can fake a profile of a user and establish connections with the victim's friends resulting in accumulating sensitive communication data. - Economic loss can be caused due to unauthorised access to data of users in OSNs (Tuunainen, Pitkanen, & Hovi, 2009).
- Data aggregation is possible for malicious users and third party applications (Acquist et al., 2007).
- Reputation jeopardy of users, especially for prospective employer (Rosenblum, 2007). - Hacking and phishing of personal data by third parties (Debatin, Lovejoy, Horn, & Hughes, 2009).
- OSNs profile pictures can be improperly used. For example, a personal profile photo from Facebook was publicly used to announce the death in the media (ABC Media Watch, Filleting Facebook. Australian Broadcasting Corporation (ABC), 29 October 07, 2007).
- OSNs-targeting worms that turns users machines into zombies on a botnet (New MySpace and Facebook Worm Target Social Networks, 2008).
- Cyberbullying and stalking by acquiring sensitive data about the victim user (Acquisti et al., 2007).
- Unwanted linkability from photos through the tags of other users who are not the owner of the photo (Acquisti et al., 2007).
- Blackmailing users (Gross & Acquisti, 2005).
- Price discrimination (Gross & Acquisti, 2005).
- Selling data to marketing companies (Rosenblum, 2007).
- Sexual predators, especially of kids, through accessing their sensitive data on OSNs (Rosenblum, 2007).
- Face recognition of profile images available on OSNs can result in users being tracked and recognized in other contexts, e.g., traffic cameras (Acquisti et al., 2007).

All of the previously mentioned issues intensify the fundamental necessity of enhancing security and privacy protection mechanisms of OSNs. To address the unforeseen threats, finegrained ACMs are required to facilitate more control and protection over any type of data disclosed in the OSN (Masoumzadeh & Joshi, 2010). We do not explicitly suggest that access control is a solution to all the above-mentioned threats; however, guarding access to data is the first fundamental step towards privacy protection. Morover, OSNs providers, such as Facebook and MySpace, support access control models to construct better trust basis with the privacy concerned users (H. Wang & Sun, 2010).

3.2 Characteristics of Access Control for OSNs

Below, we discuss some essential characteristics [13, 14] that need to be supported in access control solutions for OSN systems.

Policy Individualization. OSN users may want to express their own preferences on how their own or related contents should be exposed. A system-wide access control policy such as we find in mandatory and role-based access control, does not meet this need. Access control in OSNs further differs from discretionary access control in that users other than the resource owner are also allowed to configure the policies of the related resource. In addition, users who are related to the accessing user, e.g. parent to child, may want to control the accessing user's actions. Therefore, the OSN system needs to collectively utilize these individualized policies from users related to the accessing user or the target, along with the system-specified policies for control decisions.

User and Resource as a Target. Unlike traditional user access where the access is against target resource, activities such as poking and friend recommendations are performed against other users. User as a target is particularly crucial for access control in OSNs since policies for users can specify rules for incoming actions as well as outgoing actions

User Policies for Outgoing and Incoming Actions. Notification of a particular friend' activities could be bothersome and a user may want to block it. This type of policy is captured as incoming action policy. Also, a user may want to control her own or other users' activities. For example, a user may restrict her own access from any violent contents or a parent may not want her child to invite her coworker as a friend. This type of policy is captured as an outgoing action policy. In OSN, it is necessary to support policies for both types of actions.

Necessity for Relationship-Based Access Control. Access control in OSNs is mainly based on relationships among users and resources. For example, only Alice's direct friends can access her blogs, or only user who owns the photo or tagged users can modify the caption of the photo. Depth is another significant parameter, since people tend to share resources with closer users (e.g., "friend", or "friend of friend").

3.3 Comparison of Access Control Models for OSNs

The first four columns of Table 1 summarize the salient characteristics of the models discussed above. The fifth column gives these characteristics for the new UURAC model to be defined in this paper.

Table 1. Comparison of Access Control Models for OSNs

	Fong [7]	Fong [8, 9]	Carminati [6]	Carminati [2, 3]	UURAC
Relationship Category					
Multiple Relationship Types		✓	✓	✓	✓
Directional Relationship		✓	✓		✓
U2U Relationship	✓	✓	✓	✓	✓
U2R Relationship				✓	
Model Characteristics					
Policy Individualization	✓	✓	✓	✓	✓
User & Resource as a Target				(partial)	✓
Outgoing/Incoming Action Policy				(partial)	✓
Relationship Composition					
Relationship Depth	0 to 2	0 to n	1 to n	1 to n	0 to n
Relationship Composition	f, f of f	exact type sequence	path of same type	exact type sequence	path pattern of different types

All the models deal only with U2U relationships, except also recognize U2R (user-to-resource) relationships explicitly. U2R relationships can be captured implicitly via U2U with the last hop being U2R. NewS\ XRTFGVB vertheless, we believe that explicit treatment of U2R and R2R (resource-to-resource) relationships is important but leave it for future work.

4. UURAC MODEL FOUNDATION

In this section, we develop the foundation of UURAC including access control model components and social graph model.

4.1 Access Control Model Components

The model comprises five categories of components as shown in Figure 1.

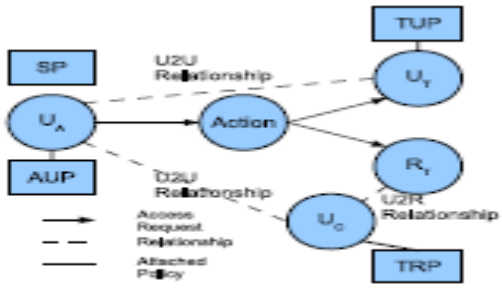

Fig. 1. Model Components

Accessing User (*ua*) represents a human being who performs activities. An accessing user carries access control policies and U2U relationships with other users. Each

Action is an abstract function initiated by accessing user against target. Given an action, we say it is *action* for the accessing user, but *action*−1 for the recipient user or resource.

Target is the recipient of an action. It can be either *target user* (*ut*) or *target resource* (*rt*). Target user has her own policies and U2U relationship information, both of which are used for authorization decisions. Target resource has U2R relationship (i.e., ownership) with *controlling users* (*uc*). An accessing user must have the required U2U relationships with the controlling user in order to access the target resource.

Access Request denotes an accessing user's request of a certain type of action against a target. It is modeled as a tuple < *ua*, *action*, *target* >, where *ua* ∈ *U* is the accessing user, *target* is the user or resource that *ua* tries to access, whereas *action* ∈ *Act* specifies from a finite set of supported functions in the system the type of access the user wants to have with *target*. If *ua* requests to interact with another user, *target* = *ut*, where *ut* ∈ *U* is the target user. If *ua* tries to access a resource owned by another user *uc*, *target* is resource *rt* ∈ *R* where *R* is a finite set of resources in OSN

Policy defines the rules according to which authorization is regulated. As shown in Figure 2,

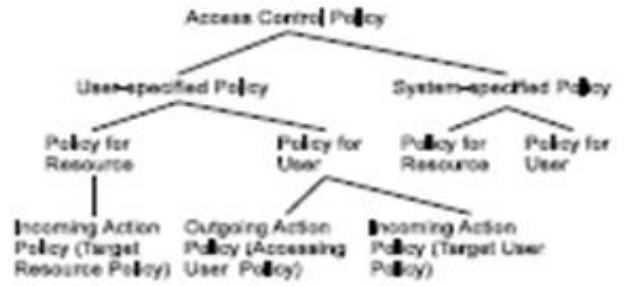

Fig. 2. Access Control Policy Taxonomy

policies can be categorized into user-specified and system-specified policies, with respect to who defines the policies. System specified policies (*SP*) are system wide general rules enforced by the **Policy** define the rules according to which authorization is regulated. As shown in Figure 2, policies can be categorized into user-specified and system-specified policies, with respect to who defines the policies. System specified policies (*SP*) are system wide general rules enforced by the **Policy** define the rules according to which authorization is regulated. As shown in Figure 2, policies can be categorized into user-specified and system-specified policies, with respect to who defines the policies. System specified policies (*SP*) are systemwide general rules enforced by the OSN system; while user-specified policies are applied to specific users and resources. Both user- and system-specified policies include policies for resources and policies for users. Policies for resources are used to control who can access a resource, while policies for users regulate how users can behave regarding an action. User-specified policies for a resource are called target resource policies (TRP), which are policies for incoming actions. User-specified policies for users can be further divided into accessing user policies (AUP) and target user policies (TUP), which correspond to user's outgoing and incoming access (see examples in Section 2.1), respectively. Accessing user policies, also called outgoing action policies, are associated with the accessing user and regulate this user's outbound access. T arget user policies, also called incoming action policies, control how other users can access the target user. Note that systemspecified policies do not have separate policies for incoming and outgoing actions, since the access or and target are explicitly identified…

4.2 Modeling Social Graph

As shown in Figure 3, an OSN forms a directed labeled simple graph1 with nodes or vertices) representing users and edges representing user-to-user relationships.e assume every user owns a finite set of resources and specifies access control policies for the resources and activities related to her. If an accessing user has the U2U relationship required in the policy, the accessing user will be granted permission to perform the requested action against the corresponding resource or user.

We model the social graph of an OSN as a triple G =< U,E,Σ >:

– U is a finite set of registered users in the system, represented as nodes (or vertices) on the graph. We use the terms user and node interchangeably from now on.

– $\Sigma = \{\sigma_1, \sigma_2, .., \sigma_n\ \sigma_{1}, \sigma^{-1}{}_2, .., \sigma^{-1}{}_n\}$ denotes a finite set of relationship types, where each type pecifier σ denotes a relationship type supported in the system.

– $E \subseteq U \times U \times \Sigma$, denoting social graph edges, is a set of existing user relationships.

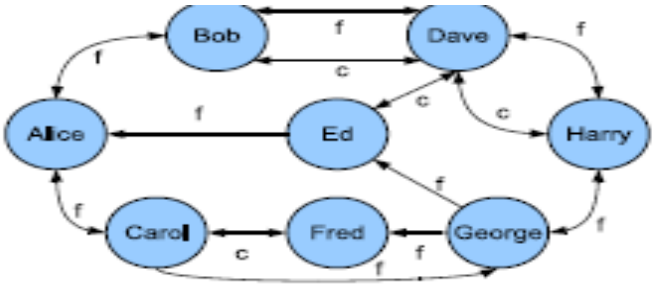

Fig. 3. A Sample Social Graph

Since not all the U2U relationships in b OSNs are mutual, we define the relationships E in the system as directed. For every σi ∈ Σ, there is $\sigma^{-1}{}_i \in \Sigma$ representing the inverse of relationship type σi. We do not explicitly show the inverse relationships on the social graph, but assume the original relationship and its inverse twin always exist simultaneously. Given a user u ∈ U, a user v ∈ U and a relationship type σ ∈ Σ, a relationship (u, v, σ) expresses that there exists a relationship of ype σ starting from user u and terminating at v. It always has an equivalent orm (v, u, σ^{-1}). G =< U, E,Σ > is required to be a simple graph.

5 .UURAC POLICY SPECIFICATIONS

This section defines a regular expression based policy specification language, to represent various patterns of multiple relationship types.

5.1 Path Expression Based Policy:

The user relationship path in access control policies is represented by regular expressions. The formulas are based on a set Σ of relationship type specifies. Each specification in this language describes a pattern of required relationship types between the accessing user and the target/controlling user. We use three kinds of wildcard notations that represent different occurrences of relationship types: asterisk (*) for 0 or more, plus (+) for 1 or more and question mark(?) For 0 or 1.

5.2 User- and System-Specified Policy Specifications

User-specified policies specify how individual users want their resources or services related to them to be released to other users in the system. These policies are specific to actions against a particular resource or user. System-specified policies allow the system to specify access control on users and resources. Different from user policies, the statements in system policies are not specific to particular accessing user or target, but rather focus on the entire set of users or resources see Table 2).

Table.2. Access Control Policy Representations

Accessing User Policy	$< action, (start, path\ rule)>$
Target User Policy	$< action^{-1}, (start, path\ rule)>$
Target Resource Policy	$< action^{-1}, r_t, (start, path\ rule)>$
System Policy for User	$< action, (start, path\ rule)>$
System Policy for Resource	$< action, r.type, (start, path\ rule)>$

In *accessing user policy*, *action* denotes the requested action, whereas (*start*, *path rule*) expresses the graph rule. Similarly, *action*−1 in *target user policy* and target *resource policy* is the passive form of the corresponding *action* applied to target user. Target resource policy contains an extra parameter *rt*, representing the resource to be accessed.

This paper considers only U2U relationships in policy specification. In general, here could be one or more controlling users who have certain types of U2R relationships with the resource and possess policies for the corresponding target resource. For simplicity, we assume the only such U2R relationship is ownership. To access the resource, the accessing user must have the required relationships with the controlling user. The policies associated with the controlling users are defined on the basis of per action per resource. For instance, when querying *read* access request on *rt*, *owner*(*rt*) returns the list of users who have ownership.

6. CONCLUSION and Future Workp

In this chapter we have reviewed the fundamental aspects of access control and the basic essential lassical ACMs. We have discussed privacy problems in OSNs and the ACMs requirements to address these problems. We have surveyed the most prominent ACMS and highlighted the main contribution of each model.

Throughout the review of ACMs, we indicated the aspects that could be extended. The discussion included models in centralized and decentralized OSNs. Finally, we proposed requirements to address the open problems in current ACMs in order to facilitate fine-grained access control and better privacy preservation in OSNs. While this work only uses user-to-user relationships for authorization, we plan to extend our model to exploit user-to-resource and resource-to-resource relationships. Improve the expressiveness of the model; we also plan to incorporate some predicate expressions for attribute-based control and filtering users and relationships.

Another future direction is to capture some unconventional relationships in OSNs, such as temporary relationships (i.e., vicinity) and one-tomany relationships (i.e., network, group). Last but not least, we will be working on implementing our approach into a prototype and doing some experiments to analyze the approach

7. REFERENCES

[1]. Abadi, M., Burrows, M., Lampson, B., & Plotkin, G. (1993). A calculus for access control in distributed systems. ACM Trans. Program. Lang. Syst., 15(4), 706–734.

[2].Acquisti, A., Carrara, E., Stutzman, F., Callas, J., Schimmer, K., Nadjm, M., et al. (2007). Security issues and recommendations for online social networks. ENISA.

[3].Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision-making. IEEE Security and Privacy, 3(1), 26–33.

[4].Ahmad, A., & Whitworth, B. (2011). Distributed access control for social networks. Information assurance and security (IAS), (p. 68-73). IEEE.

[5].systems (Tech. Rep. No. 2010-959-08). Department of Computer Science, University of Calgary, Calgary, Alberta, Canada.

[6].Baden, R., Bender, A., Spring, N., Bhattacharjee, B., & Starin, D. (2009). Persona: an online social network with user-defined privacy. In Proceedings of the ACM SIGCOMM 2009 conference on data communication (pp. 135–146). New York, NY, USA, ACM.

[7]. Bruns, G., Fong, P.W., Siahaan, I., Huth, M.: Relationship-based access control: its expression and enforcement through hybrid logic. In: ACM CODASPY (2012)

[8]. Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M., Thuraisingham, B.: A semantic web based framework for social network access control. In: ACM SACMAT 2009)

[9]. Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M., Thuraisingham, B.Semantic web-based social network access control. Computers and Security 30(2-3) (2011); Special Issue on Access Control Methods and Technologies

[10]. Carminati, B., Ferrari, E., Perego, A.: Rule-Based Access Control for Social Networks.In: Meersman, R., Tari, Z., Herrero, P. (eds.) OTM 2006 Workshops, Part II. LNCS, vol. 4278, pp. 1734–1744. Springer, Heidelberg (2006)

[11]. Carminati, B., Ferrari, E., Perego, A.: A decentralized security framework for webbased social networks. Int. Journal of Info. Security and Privacy 2(4) (2008)

[12]. Carminati, B., Ferrari, E., Perego, A.: Enforcing access control in web-based social networks. ACM Trans. Inf. Syst. Secur. 13(1) (2009)

8. BIOGRAPHIES

Mr. sreenu Banoth received the M.tech degree in Medical Image and Image Analysis from IIT KHARAGPUR University, India in 2009 and had 9 year of teaching and one year industry experience. Presently working as an Asst. professor, department of CSE, WWARANGAL INSTITUTE OF TECHNOLOGY ANDD SCIENCE, WARANGAL. Research interest includes cloud computing, Data mining and image processing.

Mr. Biyyala Prashanth received the M.tech degree in CSE from JNTUH University, India in 2016 and had 1 year of teaching experience. Presently working as an Asst.professor, department of CSE, WWARANGAL INSTITUTE OF TECHNOLOGY ANDD SCIENCE, WARANGAL. Research interest includes Network security, Software Engineering and Data mining.