Trust-involved access control in collaborative open social networks

Hua Wang Lili Sun
Department of Maths and Computing
University of Southern Queensland
Toowoomba QLD 4350, Australia
Email:(wang, sun)@usq.edu.au

***Abstract*—This paper proposes a trust involved management framework for supporting privacy preserving access control policies and mechanisms. The mechanism enforces access policy to data containing personally identifiable information. The key component of the framework is an access control model that provides full support for expressing highly complex privacy-related policies, taking into account features like purposes and obligations. A policy refers to an access right that a subject can have on an object, based on relationship, trust, purpose and obligations. The structure of purpose involved access control policy is studied. Finally a discussion of our work in comparison with other access control and frameworks such as *EPAL* is discussed.**

***Keywords*-Purpose, Privacy, Access Control**

I. INTRODUCTION

One principle of participating web-based social network (*WBSN*) is to share and exchange information with other users including strangers [Crescenzo and Lipton, 2009]. For example, Facebook (www.facebook.com) has more than 350 million active users who are able to publish resources and to record and/or establish relationships with other users including how much they trust people. As the number of users and the number of sites themselves explode, securing individuals privacy to avoid threats such as misuse becomes an increasingly important issue [Liu and Terzi, 2009]. An example of misuse is that users happen to share various types of sensitive data which trigger undesired consequences of job firing (Popkin, H.: Twitter Gets you Fired in 140 Characters or Less (March 23, 2009), http://www.msnbc.msn.com/id/29796962). Indeed, Facebook receives the complaints of informing users with the latest personal information related to their online friends [Chen06]. These complaints result in an online petition, signed by over 700,000 users, demanding the company to stop this service. The fact that the sensitive message is collected and shared without any consent or awareness violates privacy for many people.

Privacy is increasing its importance since it becomes a major concern for both customers and enterprises in today's corporate marketing strategies. This raises challenging questions and problems regarding the use and protection of private message. One principle of protecting private information is based on who is allowed to access private information and for what purpose [Agrawal et al. 2002]. For example, personal information provided by patients to hospitals may only be used with record purpose, not with advertising purpose. Purposes are reasons for data collection and data access. The motivations of adopting purpose are 1) the fundamental policies for private information concern with which data object is used for what purposes (for example, customers' age and email address are used for the purpose of marketing analysis), and 2) customers agreed data usage varies from individual to individual. Information technology provides the capability to store various types of users' information required during their business activities. Indeed, Pitofsky [2000] showed that 97 percent of web sites were collecting at least one type of identifying information such as name, e-mail address, or postal address of consumers.

Data privacy is defined by policies describing to whom the data may be disclosed and what are the purposes of using the data [Abiteboul and Agrawal 2005]. For example, a policy may specify that price of an air ticket from an agent may be disclosed, but only with "opted-in" customers, or that the price will be disclosed unless the agent has specifically "opted-out" of this default. While there is recent work on defining languages for specifying privacy policies [Schunter et al. 2003, Cranor et al. 2006], access control mechanisms for enforcing such policies have not been investigated [LeFevre et al. 2004]. Ni et al. [2007] analysed a conditional privacy management with role based access control, which supports expressive condition languages and flexible relations among permission assignments for complex privacy policies. But many interested problems remain, for example, developing a formal method to describe and manage access control policy with purposes. As stated by Adams and Sasse (2001): "Most invasions of privacy are not intentional but due to designers' inability to anticipate how this data could be used, by whom, and how this might affect users"?

Trust plays a key role when performing access control in social network since it is one of the fundamental parameters to decide whom can share information, from whom can accept information [Golbeck, 2009]. A trust model for *WBSN* should keep into account that, in this scenario, the semantics of trust should be also related the compliance with the specified access control policies and privacy preferences.

Another important point is how to compute trust. Indeed, it is quite evident that assigning a wrong trust value to a potential malicious user could imply unauthorized releasing of information or unauthorized disclosure of personal relationships. Liu and Terzi (2009) analysed trust involved privacy scores of users in Online Social Networks. The area of trust modelling, computation and protection in collaborative communities is new and therefore a lot of research issues still remain open. We adopt the trust definition and do not discuss trust models since it is out of the scope of the paper.

Approaches, such as password protection, have nearly always been available for standard web pages, blogs, webmail, and bulletin boards. However, as aspects of Web 2.0 continue to be adopted, the ability to protect information within the same page will be required. For example, a blogger might maintain a single blog, but wish to control access to particular entries based on the reader's relationship to the blogger. The ability to perform this type of fine-grained access control will not only become essential in the world of Web 2.0, it will largely determine the success or failure of many social, political, and economic realms in the Web 2.0 world. Access control and the related privacy issues is a new research area and only few work have been done in this field. Indeed, most of today WBNSs enforce access control according to a very simple model (referred as basic in Table 1), according to which the owner of a resource has only 3 options wrt its protection: 1) defining it as public, 2) defining it as private, or 3) defining it as accessible only by his/her direct neighbours. Examples of *WBSN*s adopting this model are FaceBook, MySpace, and LinkedIn. Some *WBSN*s enforce variants of the basic model, in order to give more flexibility, but the principle is the same. All these approaches have the advantage of being easy to be implemented, but they lack in flexibility in terms of the access control requirements that can be specified. This paper will design a fine-grained access control scheme for social network.

The remainder of this paper is organized as follows: Section 2 presents the motivations behind our work in this paper. We find that both purpose-based access control for privacy preserving in social network and the analysis of access control policies have not been widely studied in the literature. Section 3 proposes a trust involved purpose based access framework which includes detailed information of trust, relation type, purposes and so on. Section 4 provides access control policy structure and authorization models as well as illustrates the impact of generating a new access policy through examples. Section 5 compares the work in this paper and related previous work, the comparisons demonstrate the significance of the work in this paper. Finally, the conclusions and futher work are given in Section 6.

II. MOTIVATIONS

The direct victims of privacy violations are consumers, but many enterprises and organizations are deeply concerned about privacy issues as well. By demonstrating good privacy practices, many companies, such as FaceBook and MySpace, try to build solid trust with customers, thereby attracting more customers. This paper provides theory and a practical demonstration of how to protect reliably and strongly private information in *WBSN.*

Suppose, for instance, that Alice is the owner of a set of resources RA, and that she wishes to share them with some of her friends. In this simple scenario, traditional access control like *RBAC* fit very well [wang et al. 2008]. Indeed, since an access control policy basically states who can access what and under which modes, and since Alice knows a priori her friends, she is able to set up a set of authorizations to properly grant the access only to (a subset of) her friends. However, if we consider a more general scenario, the traditional way of specifying policies is not enough. For instance, let us suppose that Alice decides to make available her resources not only to her friends, but also to their friends, the friends of their friends, and so on. The problem is that Alice may not know a priori all her possible indirect friends, and thus she may not be able to specify a set of access control policies applying to them. Moreover, if we consider that relationships among users of a *WBSN* could change dynamically over time, this solution implies a complex policy management. An access control model for *WBSN*s should therefore take into account that usually a node in the network wishes to share its data with other nodes on the basis of both direct and indirect relationships existing among them. Thus the data owner can control the release of their personal information in the same manner he would control it in the analog world– based on their relationship with the data receiver rather than the receiver's role. One result is that people can hold multiple relationships with someone (e.g., both sister and close friend), and can even be present in what might be considered to be conflicting relationships (e.g., a mother might generally be considered to be a friend, yet a daughter might not want to reveal everything she reveals to her friends to her mother as well). Some social networking sites, such as FaceBook (http://www.facebook.com), have started to develop these forms of control, however the relationships that they can represent are still limited.

Let us consider again the *WBSN* depicted in Figure 1, and assume once again that Alice wishes to share her data with some of her direct and indirect friends. In particular, she wants to grant access to Bob (B) and Colon who are direct friends of hers. She wants to allow also Dave to access her data, even if Alice does not know them directly, because they are direct friends of Bob and Colon. In contrast, Alice may not want to give Emma (E) access to her resources,

WBSN	Purpose	Relatinoship	Trust	Protection
FaceBook	general	friend	none	basic
Myspace	general	friend	none	basic
LinkedIn	business	various(colleague, classmate, friend)	business	limited length connection

Table I
WBSNS COMPARATIVE INFORMATION

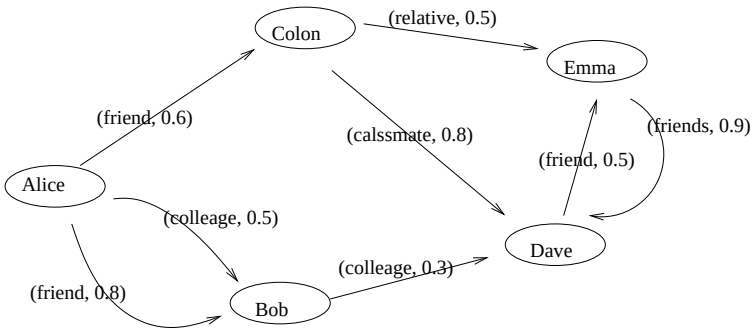

Figure 1. Type and trust level of relationships

since she does not know how Dave chooses his friends. In conclusion, when considering a *WBSN*, the length of the path connecting two nodes (i.e., the depth of a relationship) is a relevant information for access control purposes. Thus, an access control model for *WBSN*s should make a user able to state in a policy not only the type but also the maximum depth of a relationship.

Although the notions of depth and trust may be related, they are not equivalent. For instance, let us suppose that Alice does not trust Bob very much, and that, in contrast, she considers Colon highly trustworthy. In this case, the depth of the relationship is the same for both Bob and Colon, but the trust level is different. Therefore, access control policies should support also constraints on the minimum trust level of a relationship.

Social network security is becoming a more and more relevant research topic [Carminati et al, 2008], two position articles recognize the relevance of addressing access control issues in *WBSN*s. In particular, Gates (2007) describes relationship-based access control as one of the new security paradigms that addresses the requirements of the so-called Web 2.0. Whereas Hart, Johnson and Stent (2007) identify content-based and relationship-based access control as the key requirements for protecting *WBSN* resources which makes use of relationship information available in *WBSN*s for denoting authorized subjects. However, those articles do not address access control and privacy requirements enforcement, an issue that is fundamental to make any security solution usable in real-world scenarios. For example, only direct relationships are considered in Hart et al. [2007], and the notion of trust level is not taken into account as one of the possible parameters to be used in access authorizations. As far as privacy is concerned, research on this issue is currently focusing mainly on privacy preserving data mining techniques that allow social network analysis without disclosing possible sensitive information.

Ali et al. [2007] adopt a multi-level security approach, where trust is the only parameter used to determine the security level of both users and resources. More precisely, to each user u a reputation value $r(u)$ is assigned, computed as the average of the trust ratings specified for him/her by other users in the system. Furthermore, Ali et al. [2007] consider only direct trust relationships, whereas we consider (a) both direct and indirect relationships, and (b) both purpose and obligations. This has the advantage of giving resource owners the ability to specify more flexible policies, making them able to better denote the constraints to be satisfied by users in order to access a resource. Kruk et al. [2006], is primarily a FOAF-based distributed identity management system for social networks, where access rights and trust delegation management are provided as additional services. Kruk et al. [2006] discuss only generic relationships, corresponding to the ones modeled by the foaf. Finally, Kruk et al. [2006] do not discuss the case of multiple policies associated with the same resource, whereas our model supports the possibility of combining policies by using the AND and OR Boolean operators.

The important techniques for private information happen within distributed systems specifically tailored to support privacy policies, such as the well known P3P standard [Cranor 2006]. In particular, Agrawal et al. [2002] introduced the concept of Hippocratic databases, incorporating privacy protection in relational database systems. An important feature of their work is that it uses some privacy metadata,

consisting of privacy policies and privacy authorizations stored in privacy-policies tables and privacy-authorizations tables respectively. However, they neither discussed the concepts of purpose with hierarchy structure, nor the prohibition of purpose and association of purposes and data elements. LeFevre, et al. [2004] presented an approach to enforce privacy policy in database systems. They introduced two models of cell level limited disclosure enforcement, namely table semantics and query semantics, but did not consider access control management. Ni et al. [2007] analysed a role-based access model for purpose-based privacy protection, but their work did not consider usage access management and the conflicts between purposes in policies. The development of access technology entails addressing many challenging issues, ranging from modelling to architectures, and may lead to the next-generation of access management. This paper develops purpose based access technology for privacy violation challenges including complex policy structured models with access control.

This paper focuses exclusively on how to specify and enforce policies for authorizing purpose-based access management using a rule-based language. We propose a comprehensive framework for purpose and data management where purposes are organized in a hierarchy. In our approach each data element is associated with a set of purposes, as opposed to a single security level in traditional secure applications. Also, the purposes form a hierarchy and can vary dynamically. These requirements are more complex than those concerning traditional secure applications. To provide sufficient functions with the framework, this paper analyses the explicit prohibition of purpose and the association of a set of purposes with access control policies. This kind of analysis for purpose-based usage control for privacy preserving has not been studied.

III. A TRUST BASED ACCESS FRAMEWORK

This section analyses the terminology included in a trust-based access framework *TBAF*. *TBAF* includes privacy-aware access control and supports trust-based information sharing and granularity of data labelling by introducing personal relationship, sticky policy in social network, fine-grained format and trust modeling.

Trust in a person is a commitment to an action based on a belief that the future actions of that person will lead to a good outcome [Golbeck, 2009]. For instance, Alice trusts Bob regarding email if she chooses to read a message (commits to an action) that Bob sends her (based on her belief that Bob will not waste her time). There are three main properties of trust that are relevant to the development of algorithms for computing it, namely, transitivity, asymmetry, and personalization.

The primary property of trust that is used in our work is transitivity. Trust is not perfectly transitive in the mathematical sense, that is, if Alice highly trusts Bob, and Bob highly trusts Chuck, it does not always and exactly follow that Alice will highly trust Chuck. It is also important to note the asymmetry of trust. For two people involved in a relationship, trust is not necessarily identical in both directions. For example, employees typically say they trust their supervisors more than the supervisors trust the employees. One property of trust that is important in social networks and has been frequently overlooked in the past is the personalization of trust. Trust is inherently a personal opinion. Two people often have very different opinions about the trustworthiness of the same person.

A trust relationship is usually modeled as a directed edge, connecting two entities A and B, labeled with information stating whether, and, possibly, how much, A considers B trustworthy. The directed edge models a specific property of trust, i.e., its asymmetric nature. In fact, if A trusts B, it does not necessary follow that B trusts A.

The data structure of *WBSN* is a tuple *(VSN, ESN, RTSN,* ϕ_{SN} *)*, where RTSN is the set of supported relationship types, *VSN* and $ESN \subseteq VSN \times VSN \times RTSN$ are, respectively, the nodes and edges of a directed labeled graph $(VSN, ESN, RTSN)$, whereas $\phi_{SN} : ESN \rightarrow [0,1]$ is a function assigning to each edge $e \in ESN$ a trust level T, which is a rational number in the range [0, 1].

An edge $e = vv' \in ESN$ expresses that node v has established a relationship of a given type rt, $e \in RTSN$ with node v'. We say that such relationship, denoted $rt(v, v')$, is direct, since v and v' are directly connected by edge e. As an example, consider the *WBSN* depicted in Figure 1, where *Alice (A)* has a direct relationship of type *friend* and trust level 0.6 with *Colon (C)*.

Note that, in a given *WBSN*, multiple paths may exist between two nodes, denoting the same type of relationship. For instance, in the *WBSN* depicted in Figure 1, three paths exist from Alice to Dave (D) denoting a relationship of type friendOf – namely, ABD, ACD, and ACED. Trust computation is more accurate when only the shortest paths are taken into account. As such, we adopt this approach throughout the project. Therefore, we extend the notion of relationship by saying that a relationship $rt(v, v')$ is the set of all the shortest paths from v to v' consisting of edges labeled with relationship type rt.

A possible solution is to adopt the same rational applied in the real world: the trust value assigned to a person is estimated on the basis of his/her reputation, which can be assessed taking into account the person behaviour. Indeed, it is a matter of fact that people assign to a person with unfair behaviour a bad reputation and, as a consequence, a low level of trust. Thus, a possible solution is to estimate the trust level to be assigned to a user in a collaborative community on the basis of his/her reputation, given by his/her behaviour with regards to all the other users in the community. In our scenario, this can be done by making a user able to monitor the behaviour of the other users wrt the release of private

information or resources. However, this solutioraises serious privacy concerns, because a participant might not agree in releasing information about the decisions he/she has made, even if these are signals of good behaviour.

Purpose: A purpose describes the reason(s) for data collection and data access [Ni et al. 2007]. A set of purposes *P*, is organized in a tree structure, referred to as a Purpose Tree *PT*, where each node represents a purpose in *P* and each edge represents a hierarchical relation (i.e., specialization and generalization) between two purposes. Figure 2 gives an example of a purpose tree.

Let P_i and P_j be two purposes in a purpose tree. P_i is senior to P_j (or P_j is junior to P_i) if there exists a downward path from P_i to P_j in the tree. Based on the tree structure of purposes, the partial relationships between purposes are existed. Suppose *PT* is a purpose tree and *P* is a set of purposes in *PT*. $Pu \in P$ is a purpose, the senior purposes of Pu, denoted by $Senior(Pu)$, is the set of all nodes that are senior to Pu. For example, *Senior(Record)* = {*Admin, General Purpose* } in Figure 2. The junior purposes of Pu, denoted by $Junior(Pu)$, is the set of all nodes that are junior to Pu. For instance, *Junior(Admin)*= {*Advertise, Record*}.

Intended purposes are purposes associated with data and thus regulate data accesses. *Access purposes* are purposes for accessing data. An intended purpose consists of two components: Allowed Intended Purposes (*AIP*) and Prohibited Intended Purposes (*PIP*), i.e. $IP = \langle AIP, PIP \rangle$, where *AIP* $\subset$ *P*, and *PIP* $\subset$ *P*. Intended purposes can be viewed as brief summaries of privacy policies for data. When an access is requested, the access purpose is checked against the intended purposes for the data item. That is, access is granted if the access purpose is entailed by the *AIP* and not entailed by the *PIP*; in this case we say the access purpose is compliant to the intended purpose. On the other hand, the access is denied if either of these two conditions fails. The access purpose is then not compliant to the intended purpose. The structure of *AIP* and *PIP* allows more compact and flexible policies in the designed model. Moreover, conflicts between *AIP* and *PIP* for the same data element are resolved by applying the denial-takes-precedence policy where *PIP* overrides *AIP*.

Let *IP* = $\langle AIP, PIP \rangle$, the set of purposes implied by *IP* is defined as
IP^* = $(Junior(AIP) \cup AIP) - (Senior(PIP) \cup PIP)$.
The advantages of this definition are: it is reality that an access purpose is compliant to $\langle AIP, PIP \rangle$ if it is compliant to $\langle Junior(AIP), PIP \rangle$. Furthermore, an access purpose is not compliant to $\langle AIP, Senior(PIP) \rangle$ if it is not compliant to $\langle AIP, PIP \rangle$.

Most privacy policies are in two categories. One is a permissive policy that selectively allows data access for a set of purposes. The other one is a prohibitive policy that explicitly prohibits access to data for certain purposes. For example, a company decides not to use any information about children of age under 13 for the marketing purpose. This policy is prohibitive in nature as it explicitly disallows access to the data items belonging to minors for the particular purpose.

IV. Access control policies

We introduce the structure of access control policy. Let us assume a social network system that possesses data or resources that need to be protected from unauthorized accesses. Policies are defined to apply to this system.

Definition 4.1 An access control policy (rule) is a tuple of the form

$$(Data, Sub, RelT, Purp, Dmax, Tmin, Obli)$$

The subjects (*Sub*) terms identifies a user or a group who requests an action onto the resources. The resources (*Data*) term identifies a subset of objects which are normally private information that access to the objects is restricted. The purpose (*Purp*) is selected a pre-defined set of purposes that is reasons subjects intend to execute an action. The *RelT* is a relationship type between the data owner and the user may have the right to access. *Dmax* and *Tmin* are maximal depth and minimal required trust respectively. Obligations (*Obli*) are requirements that have to be followed by the subject for having access to resources. For instance, users are asked to agree to a privacy policy when installing Skype software; otherwise, the software cannot be used.

Subjects, relationship type, and trust are the same concepts in traditional access control policies that specify who can access what with action. Purposes are applied to achieve fine-grained polices. The purpose checks for properties of the context with no intended side effects. If a side effect exists we need to consider other arguments like obligations and conditions in authorization process. We briefly discuss obligations in this paper but the detailed analysis for obligations is omitted. As we mentioned in the first section, the purpose is the reason to collect the resources and is indispensable to private access policies.

Access control requirements applying to a resource are expressed by specifying one or more access conditions, by which the resource owner Sub determines the type of relationships that a requesting node R must have with a given node along with access purpose, their maximum depth, minimum trust level and obligations. A privacy policy, $\langle Data, Sub, RelT, Purp, Dmax, Tmin, Obli \rangle$, describes the data disclosed to whom must have a relationship, $RelT \in RTSN \cup *$ is a relationship type, whereas $Dmax \in N \cup *$ and $TMmin \in [0, 1] \cup *$ are, respectively, the maximum depth and minimum trust level that the relationship must have and satisfy obligations. If $Sub = *$ and/or $RelT = *$, Sub corresponds to any node in V_{SN}/or $RelT$ corresponds to any relationship in RT_{SN}, whereas, if $Dmax = *$ and/or $Tmin = *$, there is no constraint concerning the depth and/or trust level, respectively.

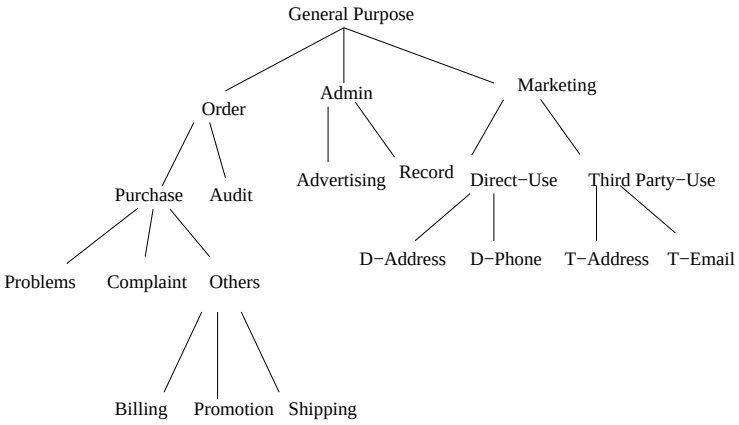

Figure 2. Example of purpose structure

Consider the *WBSN* depicted in Figure 1, suppose that Alice owns her email address that should be accessed by users that are either friends of Alice with purpose of purchase, constraints on depth 3, trust level 0.8 or direct colleagues of Carl with marketing purpose, independently from their trust level. This can be achieved by specifying two distinct access rules, namely, $(EmailAddress, Alice, Friends, Purchase, 3, 0.8, \phi)$ and $(EmailAddress, Carl, colleague, Marketing, 1, 0, \phi)$.

The following two examples are positive and negative authorizations, respectively. The security policy example includes two rules.

Example 1: "Hua allows his direct friends with minimal 0.8 trust to access his address for marketing purpose by notify through email";

Example 2: "Chris does not allow colleague to access his home phone for record purpose".

In the first rule *Data = Address, Sub = Hua, RelT = friends, Purp = Marketing, Dmax = 1, Tmin = 0.8, Obli = Notify (email)*. The second example with negative authorization, *Data = Home phone, S = Chris, RelT = Colleague, Purp = record, Dmax = 0, Tmin = 1*. Due to the negative policy, we set up the Dmax to 0. There is no obligations in the second example. Therefore,

P1: (Address, Hua, Friends, Marketing, 1, 0.8, Notify (Email))

P2: (Homephone, Chris, Colleague, Record, 0, 1, ϕ)

A. Policy operations

This section analyses the impact of generating new policies to an existing Trust-based access control (*TAC*) model. It may have unforeseen problems while a new policy for privacy protection is raised. For example, when Hua moves to the complaint department, a new policy is defined:

3. "Hua allows his direct friends with minimal 0.8 trust to access his address for problem solving purpose by notify through email";

The corresponding expression in *TAC* is:

P3: (Address, Hua, Friends, problem solving, 1, 0.8, Notify (Email)).

Comparing to P1, these are two policies for people access Hua address for different purposes. What is the results of these two policies if combine them together? Normally, we should apply P1 for access address for Marketing purpose and, apply P3 to access address for Problem solving purpose.

The differences in these two policies are the purposes where one is Marketing purpose while the other one is Problem Solving purpose. How the system will verify?

Should the system verify Marketing purpose for the access to addresses with consent conditions? *TAC* achieves that by considering different access policies as linked by a conjunction.

That is, if a user Sub allows to others with relationship type *RelT* and minimal trust *Tmin* to access on *data* for purpose $Purp$, all access polices of Sub related to the data, Depth, Trust, Purposes and Obligations must be checked. Sub can read the *data* if there exists at least one policy and Sub can satisfy all purposes in all policies. If a new access policy is related to the same data, same obligations of some existed private policies, it is not used to relax the access situations but to make the access stricter. If privacy officers want to relax the access environments, they can do so by revising the existed access policies instead of creating a new one.

"Obligations" are requirements that have to be followed by the subject for allowing access resources. For instance, users are asked to agree a privacy policy when install Skype software; otherwise, the software cannot be used.

Consider the following access policies which include conflicting obligations:

P4: (Homephone, Chris, Colleague, Record, 2, 1, Notify())

P5: (Homephone, Chris, Colleague, Record, 2, 1, Notify(Opt-out))

Once a data request is authorized, the system does not know which obligation should be executed (either Notify or

Notify with Opt-out); therefore P4 conflicts with P5.

Access control architecture However, besides the definition of a suitable policy language, one of the key issues is related to the architecture according to which access control should take place. The traditional way according to which access control is performed in data management systems does not fit very well with the collaborative community scenario. In a traditional data management system, there is a trusted module, called reference monitor, which mediates each access request submitted to the system, and decides whether it can be granted or not, on the basis of the specified access control policies. The access control policies specified by all the users are stored into a centralized policy base, managed by the database server. This architecture is not appropriate for a collaborative community environment for two main reasons. The first is that in a dynamic and highly decentralized environment like collaborative communities, a centralized service in charge of performing access control may become a bottleneck for the whole system. The second reason is that adopting centralized access control enforcement implies to totally delegate to the community manager the administration of user data and the related access control policies and this may lead to some privacy and confidentiality concerns. For instance, a community user might not want that the community manager knows the policies regulating access to his/her resources. Additionally, the increasing privacy concerns about the management of personal information by the community manager lead us to believe that a centralized access control solution is not the most appropriate one, since we believe that, in the next future, collaborative community users would like to have more and more control over their data and the way access control is enforced over them.

V. Comparisons

We present a brief comparison of the trust involved access model *TAC* against other related work. The closely related works to this paper are Social Network Privacy via Evolving Access Control [Crescenzo and Lipton, 2009] and the enterprise privacy authorization language (*EPAL*)[Schunter, et al. 2003].

Crescenzo and Lipton [2009] introduced the problem of limiting privacy loss due to data shared in a social network, where the basic underlying assumptions are that users are interested in sharing data. The authors shown that users-regulated access control is unsuccessful for practical social network, and proposed that social networks deploy an additional layer of server-assisted access control which, even under no action from a user, automatically evolves over time, by restricting access to the user's data. The evolving access control mechanism provides non-trivial quantifiable guarantees for formally specified requirements of utility. Their work is different from ours in two aspects. First, their paper is focused on limiting privacy loss while participating to online activity at social networking websites. By contrast, our work has analysed trust-based access framework with different relationship types in social network. Second, their work designed a new model for balancing privacy and utility in social networks, and proposed a solution that achieves non-trivial tradeoffs between these two goals. They neither analyse the trust and depth of relationship nor purpose structure and obligations. By contrast, our work has analysed purpose hierarchical structure and the impact of adding new access control policies.

EPAL [Schunter, et al. 2003] is a formal language for writing enterprise privacy policies to govern data handling practices in IT systems according to fine-grained positive and negative authorization rights. It concentrates on the core privacy authorization while abstracting data models and user-authentication from all deployment details such as data model or user-authentication. An *EPAL* policy defines lists of hierarchies of data-categories, user-categories, and purposes, and sets of (privacy) actions, obligations, and conditions. Purposes model the intended service for which data is used (e.g., processing a travel expense reimbursement or auditing purposes). Compared to *EPAL*, *TAC* has the following major differences. First, one of the important design criteria of *TAC* is to unify privacy policy enforcement and access control policy enforcement into one access control model. By contrast, EPAL is designed independently from any access control model. Second, the conflicting policies problem was not introduced and analysed in *EPAL*; hence shortcoming exists during answering data access request [Barth et al. 2004], but *TAC* supports conflict detection to guarantee that no conflicts arise in the procedures of generating new policies, thus preventing the disclosure of private information. Third, we analyse the policy structure with trust, relationship type, purpose and obligation in social network which are not discussed in *EPAL*.

VI. Conclusions and future work

This paper has discussed trust-based access control policies with purposes and obligations. We have studied the access control framework but also the structure of access policies including subjects, resources, purposes, trust, relationship types and obligations. We have also analysed the impact of adding new policies and the conflicts that they can lead to. The work in this paper has significantly extended previous work in several aspects, for example, purpose involved access control, and access control policies in collaboration social network.

The research for trust involved access control policies is still in its infancy and much further work remains to be done. There could exist conflicting access policies within *TAC* in social network, and how to develop algorithms to find and fix the conflicts and their applications are possible avenues for our future work. The development of a system

approach to test the conflicts between policies is also being considered.

REFERENCES

[1] Abiteboul, S. and Agrawal, R. 2005. The *Lowell* database research self-assessment. *Communications of the ACM*. 48 (5),111–118.

[2] Adams, A. and Sasse, A., 2001. Privacy in Multimedia Communications: protecting users, not just data. *People and Computers XV - Interaction Without Frontiers*. Joint Proceedings of HCI2001 and ICM2001, pp. 49-64.

[3] Agrawal, R., Kiernan, J., Srikant, R. and Xu,Y. 2002. Hippocratic databases. *Proceedings of the 28th International Conference on Very Large Databases* (VLDB).

[4] Ali, B., Villegas, W. and Maheswaran, M. (2007). A trust based approach for protecting user data in social networks. Proceedings of Conference of the Center for Advanced Studies on Collaborative research (CASCON07), Richmond Hill, Ontario, Canada.

[5] Barth A., Mitchell, J.C. and Rosenstein J. 2004. Conflict and combination in privacy policy languages. *Proceedings of the ACM workshop on Privacy in the electronic society*, pages 45-46.

[6] Carminati, B., Ferrari, E., and Perego, A. 2009. Enforcing access control in Web-based social networks. ACM Trans. Inf. Syst. Secur. 13, 1 (Oct. 2009), 1-38.

[7] Chen, L: Facebooks Feeds Cause Privacy Concerns. the Amherst Student. Available at: http://halogen.note.amherst.edu/astudent/2006-2007/issue02/news/01.html, October 2006.

[8] Cranor L. et al. 2006. The platform for privacy preferences 1.1 (P3P) specification. *W3C Working Group*.

[9] Crescenzo, G. and Lipton, R. J. 2009. Social Network Privacy via Evolving Access Control. In Proceedings of the 4th international Conference on Wireless Algorithms, Systems, and Applications (Boston, MA, August 16 - 18, 2009). B. Liu, A. Bestavros, D. Du, and J. Wang, Eds. LCSN, vol. 5682. Springer-Verlag, 551-560.

[10] Gates, C. 2007. Access Control Requirements for Web 2.0 Security and Privacy. Position paper accepted to the Workshop on Web 2.0 Security and Privacy. Oakland, California, United States.

[11] Golbeck, J. 2009. Trust and nuanced profile similarity in online social networks. ACM Trans. Web 3, 4 (Sep. 2009), 1-33. DOI= http://doi.acm.org/10.1145/1594173.1594174

[12] Liu, K. and Terzi, E. 2009. A Framework for Computing the Privacy Scores of Users in Online Social Networks. ICDM '09: Proceedings of the 2009 Ninth IEEE International Conference on Data Mining, 288297. IEEE Computer Society.

[13] Golbeck, J. 2009. Trust and nuanced profile similarity in online social networks, ACM Trans. Web, vol. 3 (4), 133.

[14] Golbeck, J.2005. Computing and applying trust in web-based social networks, University of Maryland at College Park, MD, USA.

[15] Hart, R., Johnson,M. and Stent, A. 2007. More content - less control: access control in the web 2.0. In: Proceedings of the Web 2.0 Security and Privacy Workshop.

[16] Kruk, S.; Grzonkowski, S.; Gzella, A.; Woroniecki, T.; Choi, H.-C. D-FOAF: Distributed Identity Management with Access Rights Delegation. In The Semantic Web ASWC 2006, Vol. 4185; Mizoguchi, R.; Shi, Z.; Giunchiglia, F., Eds.; Springer Berlin Heidelberg: 2006.

[17] LeFevre, K., Agrawal, R., Ercegovac, V., Ramakrishnan, R., Xu, Y. and DeWitt, D. 2004. Limiting disclosure in hippocratic databases. *Proceedings of the 13th VLDB conferenc*. 108–119.

[18] Li M., Sun X., Wang H. and Zhang Y., Optimal Privacy-aware Path in Hippocratic Databases, *The 14th International Conference on Database Systems for Advanced Applications(DASFAA2009)*, April 21-23, 2009, Brisbane, Australia.

[19] Ni, Q., Lin, D., Bertino, E. and Lobo, J. 2007. Conditional privacy-aware role based access control. *ESORICS*, 72–89.

[20] Ni, Q., Trombetta, A., Bertino, E., and Lobo, J. 2007. Privacy-aware role based access control. *Proceedings of the 12th ACM Symposium on Access Control Models and Technologies*. France, 41-50.

[21] Pitofsky, R. et al. 2000. Privacy online: Fair information practices in the electronic marketplace, a report to congress, *Federal Trade Commission*.

[22] Schunter M. et al. 2003. The enterprise privacy authorization language (epal 1.1). *W3C Working Group*.

[23] Seamons, K., Winslett, M. and Yu, T. 2001. Limiting the Disclosure of Access Control Policies during Automated Trust Negotiation. *Proc. of NDSS01*. 109-125.

[24] Sun, X, Wang, H., Li, J. 2009. Injecting Purpose and Trust into Data Anonymization. to appear in The 18th ACM Conference on Information and Knowledge Management(CIKM 2009).

[25] Wang, H., Zhang Y. and Cao, J. TKDE09. Effective collaboration with information sharing in virtual universities, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 21(6), 840-853.

[26] Wang, H., Cao, J. and Zhang, Y. 2008b. Access control management for ubiquitous computing, *Future Generation Computer Systems*, Vol. 24, Issue 8, Pages: 870-878, October, 2008

[27] Wang, Y., Vassileva, J. 2003. Trust and reputation model in collaborative networks. *in Proc. 3rd IEEE Int. Conf. Collaborative Computing*. 150- 157.