World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:4, No:1, 2010

A Purpose Based Usage Access Control Model

Lili Sun, Hua Wang

***Abstract*—**As privacy becomes a major concern for consumers and enterprises, many research have been focused on the privacy protecting technology in recent years. In this paper, we present a comprehensive approach for usage access control based on the notion purpose. In our model, purpose information associated with a given data element specifies the intended use of the subjects and objects in the usage access control model. A key feature of our model is that it allows when an access is required, the access purpose is checked against the intended purposes for the data item. We propose an approach to represent purpose information to support access control based on purpose information. Our proposed solution relies on usage access control (UAC) models as well as the components which based on the notions of the purpose information used in subjects and objects. Finally, comparisons with related works are analyzed.

***Keywords*—**Purpose, privacy, access control, authorization

I. Introduction

THE rapid growth in information technology and database systems has greatly increased the need for privacy protection. Privacy becomes a major concern for consumers and enterprises, much research have been focused on developing the privacy protecting technology. Access control has been considered as a major issue in information security community since the beginning of the information security discipline. A number of privacy protecting access control models have been proposed in recent years [1]. Through access control, the system can restrict unauthorized users access to the resources in the system and guarantees the confidentiality and integrity of the resources. Traditional access control models primarily consider static authorization decisions based on the subjects' permissions on target objects. It focuses on the protection of data in a closed environment. More recently research in authorization is about trust management [20]. Trust management relates authorization to a user's capability and properties. These access models have been used on the control of access to server-side objects. Digital rights management (DRM) is used for objects disseminated [14]. Current DRM solutions are largely focused on payment-based dissemination controls. Because each of access control, the authorization decisions are generated at request time but do not consider ongoing controls for long access or for revocation. We need a comprehensive, systematic approach for controls on usage of digital objects. Recently proposed usage control is a new access control model extending traditional access control models in multiple aspects [9]. The term "usage" means usage of rights on digital objects. The main different properties of usage control with traditional access control models are continuity of access decision and mutability of subject attributes and object attributes [9]. Continuity is another decision factor in access control management. In traditional access control, authorization is assumed to be done before access is allowed (pre). However, it is quite reasonable to extend this for continuous enforcement by evaluating usage requirements throughout usages (ongoing).

In order to protect data privacy, the notion of purpose plays a major role in access control models and an appropriate metadata model was developed to support such privacy based access control models [6]. Purpose is the reasons to collect or

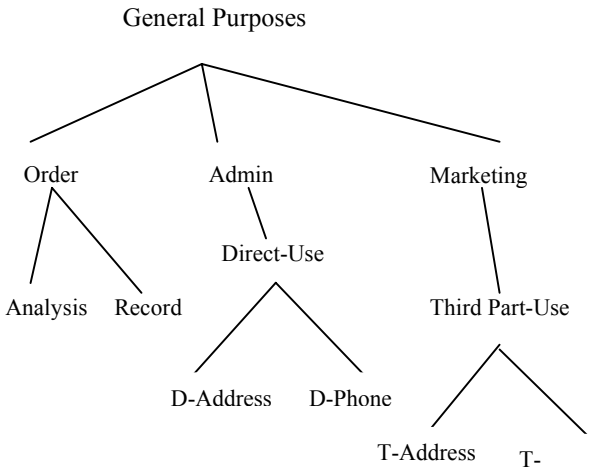

Fig. 1 Example of purpose structure

Lili Sun is with the Department of Mathematics and Computing, University of Southern Queensland, QLD 4350, Australia (corresponding author to provide phone: 61-746315527; e-mail: sun@ usq.edu.au).

Hua Wang is with the Department of Mathematics and Computing, University of Southern Queensland, QLD 4350, Australia (e-mail: wang@usq.edu.au).

to access private data in access management systems. The important techniques for private information happen within database management systems (DBMS) specifically tailored to support privacy policies, such as the well know P3P standard (W3C). In particular, Agrawal et al. [1] recently 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 sophisticated concepts of purpose with hierarchy structure, nor the prohibition of purpose and association of purposes and a data element.

Our previous work has, however, some limitations [15]. The first is that it has been developed based on XML and object-relational data model with using usage access control. But to manage purpose information that are complex, have hierarchical structures and are characterized by several semantic relationships, we need to develop a sophisticated purpose management model. The second is that does not adequately address the problem of how to determine the purpose for which certain data are accessed by a given user. We believe that this issue may be satisfactorily addressed by relying on the usage access control model. However, in order to support specifying for which purpose a certain can be accessed by a given object, we need to develop an extend usage model which is based on the purpose of subjects and objects. Such an extended UAC model has never been studied before and, the new model and its authorizations are the major contributions of this paper.

The remainder of this paper is organized as follows: Section 2 provides a brief overview of purpose and access purpose determination. The usage control model and Continuity properties are introduced in this section. Section 3 shows our proposed authorization models for usage control using purpose scheme. It includes *pre-Authorizations, ongoing-Authorizations, pre-Obligations, ongoing-Obligations, pre-Conditions and ongoing-Conditions* six models. Section 4 presents usage access control architectures based on purpose data. Section 5 reviews the differences between the work in this paper and others related works. Finally, Section 6 concludes the paper.

II. Related Technologies

A. Purpose

A privacy policy mainly concerns with which data object is used for which purposes. As the purpose directly dictates how accesses to data items should be controlled, therefore, purpose plays a central concept in many privacy protecting access control models [2]. In common business environment, purposes naturally have a hierarchical relationship among them, such as generalization and specialization relationships. Purposes can be organized according to the hierarchical relationships to simplify the management of purposes [6]. In this section, we present an overview of the notion of purpose.

A purpose describes the reasons for data collection and data access [2]. The purpose directly dictates how accesses to data items should be controlled. 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. Fig. 1 gives an example of a purpose tree. In this example, purpose "Analysis" is a specialization of purpose "Admin".

To access a specific data item should be allowed if the purposes allowed by privacy policies for the data include or imply the purpose for accessing the data[2]. 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*). For example, an intended purpose *Pu* is a tuple *(AIP, PIP)*, where $AIP \subseteq P$ and $PIP \subseteq P$ are two sets of purposes.

Intended purposes can be viewed as brief summaries of privacy policies for data. An access decision is made based on the relationship between the access purpose and the intended purpose of data. When an access is required, 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*; the access is denied if either of these two conditions fails.

B. Access Purpose Determination

An access purpose is the reason provided by subjects for accessing a data item. The system has to determine the access decision that is made directly based on the access purpose. The access decision should be dynamically determined, based on the current context of the system. For example, suppose an employee in the shipping department is requesting to access the address of a customer by using a particular application in a normal business hour. The key challenge for implementing this method is that it may be difficult to infer the access purposes accurately and efficiently. As an access purpose has a tree structure, it can be used hierarchical documents, such as XML documents. In the following section, we present a method for determining access purposes in UAC model.

We extend UAC model by adding access purposes and discuss the details of the access purpose authorization and verification based on the model. In our method, users are required to state their access purposes along with the data access requests, and system validates the stated access purposes by ensuring that the users are allowed to access data for the purposes. Access purpose authorizations are granted to users based on the access purpose on the data, obligations and conditions. We have already analysed different authorizations models in UAC such as pre-Authorization model and ongoing-Authorizations model [7], and will study purpose involved authorization for these models in this paper.

C. Usage Control

In this section we briefly review the general ideas of usage control and its authorization models. The traditional access control method normally deals only with authorization decisions on users' access to target resources. The usage control is a generalization of access control. It enriches and refines the access control discipline in its definition and cover obligations, conditions, continuity (ongoing controls) and mutability [12]. There are eight core components in the usage control model: subjects, subject attributes, objects, object attributes, rights, authorizations, obligations, and conditions (see Fig. 2). The authorization, obligations and conditions are components of usage control decisions.

In the usage control model, the authorization rule permits or denies the access of a subject to an object based on subject and object attributes. Obligations are performed by subjects or by the system. Conditions are not related to subject or object attributes. They are system environment restrictions.

In the usage control model, subjects and objects are familiar concepts with traditional access control. Subject and object attributes can be used during the access decision process. Subject attributes are identities, group names, roles, memberships, security clearance, and so on. Objects are entities that subjects hold rights on, whereby the subjects can access or use objects. For instance, in an on-line shopping store, a customer can be subject. A price could be an object attribute, for example, the soybean machine is priced at $88 and with delivery is required at $98. Rights are privileges that subjects can hold on objects. The authorizations of rights require associations with subjects and objects. A right represents the access of a subject to an object, such as read or write.

Authorizations, obligations and conditions are decision factors used to check and determine whether a subject should be allowed to access an object. Obligations and conditions are new concepts that can resolve certain shortcomings that have been in traditional access controls. In general, the authorization of most traditional access controls are assumed to be done before access is allowed. However in the usage control model it extends this for continuous enforcement. Authorizations may require updates on subject and object attributes. The process of continuity properties in usage control model consists of three phrases, before usage, ongoing usage and after usage. To enforce control decisions, we have two different types: pre-decision and ongoing-decision. For mutability, there are three kinds of updates: pre-update, ongoing-update, and post-update. Therefore, Authorizations can be either pre-authorization (preA) or ongoing-authorization (onA). Pre-authorization is performed before authorization is required to the access. But ongoing authorization may be performed during the access, such as when a book stocking list in a bookstore is periodically checked while the access is in progress.

Obligations are requirements that a subject must perform before (pre) or during (ongoing) accesses. An example of a pre-obligation is the requirement that a user must provide some contact and personal information before accessing IEEE digital library. The requirement that a user has to keep certain advertising windows open while he is accessing some service, is an example of an ongoing obligation. Conditions are decision factors that depend on environmental and system-oriented requirements. Subject and object attributes can be used to select which condition requirements have to be used for a request.

Based on the involvement of three decision factors: authorizations, obligations, and conditions, we have six possible cases as a model for usage control: pre-Authorizations, ongoing-Authorizations, pre-Obligations, ongoing-Obligations, pre-Conditions and ongoing-Conditions.

III. Access Purpose Authorization in the Usage Access Control Model

A. Access Purpose Authorization

An access decision is made based on the relationship between the access purpose and the intended purposes of data [2]. The access is granted if the access purpose is entailed by the allowed intend purposes and not entailed by the prohibited intended purposes. In this case we can say the access purpose is compliant to the intended purpose. The access is denied if any of these two conditions fails; we can say the access purpose is not compliant.

Let PT be a purpose tree and P be the set of all purposes in PT. Pu is a set of intended purposes, denoted as $Pu = (AIP, PIP)$ and AP is an access purposes defined over PT. $AIP \in P$, $PIP \in P$. AP is compliant to Pu, denoted as $AP \Rightarrow_{PT} Pu$, if the following two conditions are satisfied:

1. $AP \notin PIP$
2. $AP \in AIP$

where $A \Rightarrow B$ means B is a necessary condition for A.
Otherwise, AP is not compliant to Pu, denoted as
$AP \not\Rightarrow_{PT} Pu$

In the usage access control models, access purposes are authorized to users through subjects. As above, let PT be a purpose tree, Pu be an intended purpose in PT, S be the set of subjects in the system. An access purpose is authorized to a specific set of users by a 2-tuple (s, pu), where $s \in S$, $pu \in Pu$. Note that both the access purpose and subjects may be organized in hierarchies. For example, In Fig. 1, let Pu and AP be an intended purpose and an access propose defined based on PT.
Suppose $Pu = (\{General\ Purpose\}, \{Marketing\})$. If $AP =$ *Direct-Use*, then $AP \not\Rightarrow_{PT} Pu$ since the hierarchy structure of *Direct-Use* and *Marketing, and Marketing* $\in PIP$.
However, if $AP =$ Admin, then $AP \Rightarrow_{PT} Pu$, as $Admin \notin PIP$ and $Admin \in AIP$.

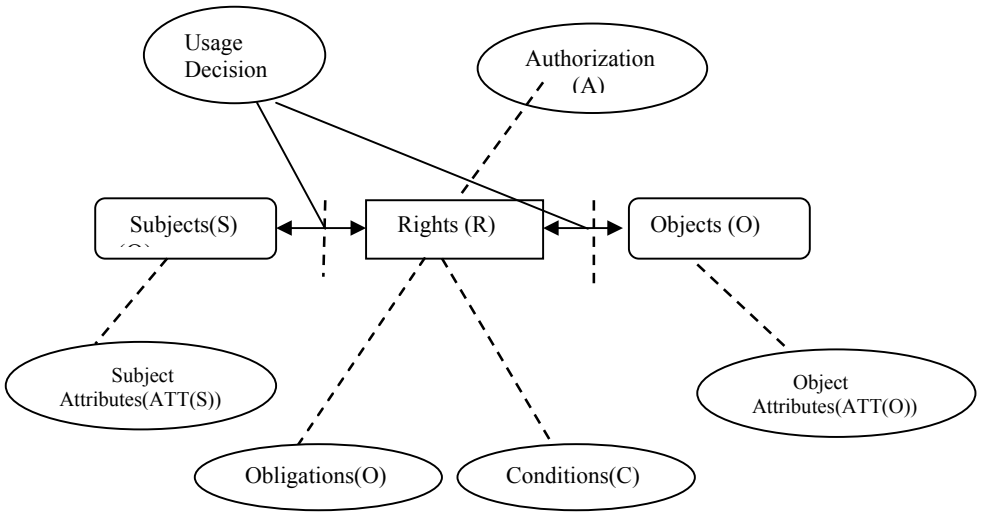

Fig. 2 Components of Usage Control Model

B. Access Purpose Authorization with Usage Access Control

In this section we consider authorization models for access purpose adopting usage control. As already discussed, usage access control includes components such as subjects, objects and obligations. The purpose involved extended usage model includes the following components:

1. A set of *S* for subjects, a set of *AP* as access purposes, a set of *O* for objects, a set *Pu = {AIP, PIP}* of purposes, a set of *R* for rights, a set of *A* for authorizations, a set of *B* for obligations and a set of *C* for conditions,

2. A set of subject with access purpose
   $SP = \{(s, ap) \mid s \in S,\ ap \in AP\}$,
   // Subject *s* with access purpose *ap*

3. A set of object with intended purpose *Pu*
   $OP = \{(o, pu) \mid o \in O,\ pu = (aip, pip) \in Pu,\ aip \in AIP, pip \in PIP\}$,

4. Object – subject assignment $SOP \subseteq SP \times OP$ is a many-to-many relation that decides what subjects with which access purposes can access the private information based on authorization.

We assume that a usage request exists on a purpose target object. Decision-making can be done either before (pre) or during (ongoing) exercise of the requested right. Decision-making after the usage has no influence on the decision of current usage. Based on the requirements we have six possible cases as a model for usage control: pre-Authorizations, ongoing-Authorizations, pre-Obligations, ongoing-Obligations, pre-Conditions and ongoing-Conditions. Depending on the access requirements on the objects in the real world, it is possible to utilize more than one case. In this paper, we consider only the cases consisting of Authorizations, Obligations or Conditions alone with pre or ongoing decisions. Meanwhile we focus on developing the usage control models for the access purpose documents.

1). Usage control for pre-Authorization Model (UCMpreA)

In a pre-Authorization usage control model, the decision process is performed before access is allowed. The following illustrations of usage decision that can be expressed on the objects are made in pre-authorizations. Before pre-authorization process, we need to decide whether the access purpose is compliant or not.

The UCMpreA model consists of the following components: *S, O, R, ATT(S), ATT(O)*, and usage decision Boolean functions *preA* on *O*, respectively, where *S, O, R,* represent Subject, Object and Rights required on the objects. *ATT(S), ATT(O),* represent attributes of subjects and objects respectively. *preA* is predicates about authorization functions. We use the notations of *AP, Pu, AIP* and *PIP* as mentioned before. *SOP* is a relation between *subject S* and object to *O*.

1. $S' \in SP$,
   Where $SP = \{(s, ap) \mid s \in S,\ ap \in AP\}$.
   In this example *SP* is a specific set of subjects by a 2-tuple*(s, ap)*. The access purpose *ap* could be a subset of *AP*. To simplify the discussion, we assume that *ap* is a single access purpose.

2. $O' \in OP$,
Where $OP = \{(o, pu) \mid o \in O, pu = (aip, pip) \in Pu\}$,
In this example OP is a specific set of objects by a 2-tuple (o, pu), where $o \in O$, $pu \in Pu$. That means object O with allowed intended purpose aip and prohibited intended purpose pip. Both aip and pip can be subsets.

3. Is the access purpose ap *compliant* to the intended purpose *pu*? subject S with access purpose must be satisfied ap $\Rightarrow_{PT}$ pu. If so, continue; otherwise, the access request is denied.

4. $allowed\ (S', O', r) \Rightarrow preA(ATT(S'), ATT(O'), r)$,
In this example this predicate indicates that if subject S' is allowed to access the objects O' with right r, then the indicated condition $preA$ must be true.

5. $SOP \subseteq SP \times OP$.
Where SOP is a many-to-many relationship from S to O. In our model, we use SOP to specify what subjects with which access purpose can access the private information objects based on authorization.

The *UCMpreA* model provides an authorization method on whether a subject can access the purpose objects. The $allowed(s', o', r)$ predicate shows that subject s' can access the object o'. At this process, the object data is assumed as private information which is restricted to access.

2). Usage control for ongoing Authorizations Model (UCMonA)

A usage control model for ongoing-Authorizations model is used to check ongoing authorizations during access processes. In this model, usage requests are allowed without any 'pre' decision making.

The *UCMonA* model has the following components: S, O, R, $ATT(S)$, $ATT(O)$, and SOP as before, and ongoing usage decision functions onA on O. onA is used to check whether S can continue to access or not.

1. $S' \in SP$,
Where $SP = \{(s, ap) \mid s \in S,\ ap \in AP\}$,
This is the same as those in pre-Authorization model.

2. $O' \in OP$,
Where $OP = \{(o, pu) \mid o \in O, pu = (aip, pip) \in Pu\}$,
This is the same as those in pre-Authorization model.

3. ap $\Rightarrow_{PT}$ pu and $allowed\ (S', O', r) \Rightarrow true$,
// Access purpose ap of subject s is compliant to the intended purpose pu of the object and S' is accessing O' with permission r. These are two prerequisites for ongoing authorization on object o.

4. $stopped\ (S', O', r) \Rightarrow \neg onA(ATT(S'), ATT(O'), r)$,
The access of subject s to o is terminated if the ongoing authorization onA is failed.

5. SOP $\subseteq$ SP $\times$ OP.
The relationship is the same as those in pre-Authorization model.

In this model usage decision Boolean functions are onA instead of $preA$. During this process the requested access is always allowed as there is no pre-authorization all the time. The access purpose ap has to be compliant to the intended purpose pu and allowed (s', o', r) is required to be true, otherwise ongoing authorization should not be initiated. Ongoing authorizations are active throughout the usage of the requested right, and some requirements are repeatedly checked for a continued access. These checks are performed periodically based on time or event. In the process when attributes are changed and requirements are no longer satisfied, stopped procedures are performed. Stopped (s', o', r) indicates that right r of subject s' on object is revoked and the ongoing access terminated. For example, a limited number of simultaneous usage, suppose only two administration staff can access the information about the price of sold books in an object o' simultaneously. If a third administration staff requests access and passes the pre-authorization, the staff with the earlier time access is terminated. While this is a case of ongoing authorizations, it is important that the certificate should be evaluated in a *pre* decision.

Due to the length of the paper, other authorization models are omitted. In practice, the six models pre Authorizations, ongoing-Authorizations, pre-Obligations, ongoing-Obligations, pre-Conditions and ongoing Conditions may need to be combined for an access control. We obtain an authorization method for the objects by checking users' (subjects') authorizations, obligations and conditions with continuity properties.

The objects usually have regular data and sensitive data. For the regular data, they do not have intended purpose, but for the sensitive data, they may have intended purpose. The following algorithm is based on these models and introduces how to manage an document access control when a user (subject) applies to access a intended purpose object with right r. The output of an access control decision is required to satisfy intended purpose object. Since the authorization process can remove some parts of the input object, the output may not satisfy some particular objects, which are required by most applications. In this case, the access will be denied.

Purpose based Algorithm:

Input: Subject s needs to access right on object o with access purpose (ap), the object o has intended purpose (pu) where pu =(aip, pip)
Output: Accesses accept or deny

Method:
1) //Verify the compliance between ap and pu
If ap ∈ aip and ap ∉ pip go to the next step; otherwise the access purpose is not compliant and the ACCESS is denied.
2)endif
3)//Verify UCMpreA
4)if preA(ATT(s), ATT(o), r) = false
//The process in pre-Authorization is not successful
5)ACCESS denied;
6)endif;
7) SOP ⊆ SP × OP
// subjects with the access purpose can access the private information
8) ACCESS accepted
// Verify UCMonA:
9) **if** *preA(ATT(s), ATT(o), r)* = false
// The process in pre-Authorization is failed, don't need further verification.
10) Application denied;
11) **endif**;
12) **if** ap $\neq>_{PT}$ pu
// *ap* is not compliant to *pu* any longer
13) Application denied;
14) **endif**;
15) **if** *onA(ATT(s), ATT(o), r)* = false
16) ACCESS stopped;
17)**endif**
18)SOP ⊆ SP × OP
// subjects with the access purpose can continue to access the private information

IV. UAC Architectures on Access Purpose Authorization

In this section, we discuss a structure of UAC architectures based on access purpose authorization. Following Fig. 3 shows the implementation layout based on our proposed architecture presented in Section 3. An access control framework consists of Usage Decision Facility (UDF) and Usage Enforcement Facility (UEF). Each facility includes several functional modules. UDF includes authorization, condition and obligation decision modules. When a subject sends an access request through UDF to the Authorization module, the Authorization module verifies the authorization process and checks whether the request is allowed or not.

The condition module is used to make a decision for whether the conditional requirements are satisfied or not. The Obligation module is applied to verify whether obligations have been performed or not before or during the requested usage. The entire messages transported among the services are identified in purpose data.

In order to build a usage access control with the notion purpose, we must consider the subjects and objects in this model with access purposes. The system has to make decision by using access purpose (AP). In this model, an access decision for the subjects and objects is made based on the compliance between the access purpose *ap* and the intended purpose *(aip, pip)* of the object.

There are purpose subjects and purpose objects. Subjects access the objects based on usage access control. When an access is required, the access purpose is checked against the intended purposes for the data item by using the comparisons of the access purpose to the allowed intended purpose and the prohibited intended purpose. The relationship between subjects and objects belongs to *SOP*. In our model, we use *SOP* to specify what subjects with which access purposes can access the private information based on authorization.

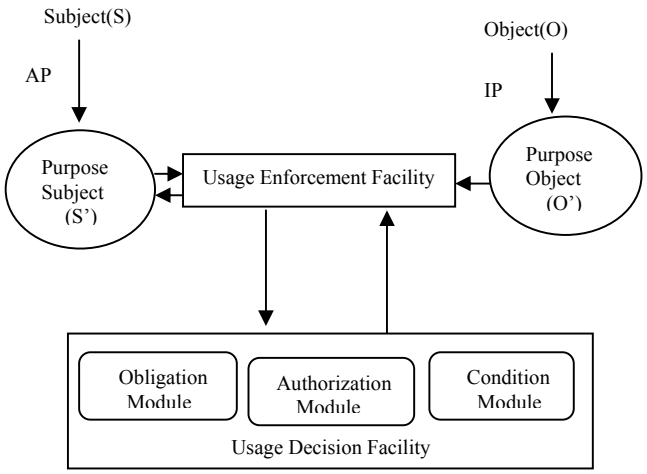

Fig. 3 UAC Architectures on Access Purpose Authorization

V. Related Work

Our work is related to many areas of privacy preserving access control, specially private data management system. We also exploit the tremendous work carried out for usage access control which mainly focuses on secure management of data.

Recently, Byun, Bertion and Li [2] introduced a purpose-based access control suited for hierarchical data. Their work focuses on how to determine the purpose for which certain data are accessed by a given user. Their proposed solution relies on the well-known role based access control (RBAC) model as well as the notion of conditional role which is based on the notions of role attribute and system attribute. It supports data access control based on the purpose information. However, our work substantially differs from that proposal. The main differences in our approach are in the following aspects. Firstly, their protocol is based on RBAC and hence it focuses on permissions-role assignment, objects hierarchies and constrains. Our approach is based on usage control, we have analysed the characteristics of various access authorizations and presented detailed models for different kinds of authorizations. Secondly, their approach does not mention how to update users' permissions on the objects when their conditions or obligations have changed. It is an

important state for the data in the Internet since users always alter their conditions or obligations. By contrast, users in our scheme have to pass pre-Authorizations and ongoing-Authorizations as well as pre-Obligations, pre-Conditions and ongoing-Obligations and ongoing-Conditions. This indicates that our method is much more powerful in dynamic environments.

Previous work we used to focus on using usage access control methods with XML document [13]. In the authorization models, the subjects and objects for access control are elements of XML documents. We did not provide the access control models based on the purpose information. Also, Elisa and Elena [3] presented an access control system supporting selective distribution of XML documents among possible large user communities by using a range of key distribution methods. In their papers, a formal model of access control policies for XML documents is given. It focuses on key distribution methods to protect XML documents. The approach consists of encrypting different portions of the same document according to different encryption keys, and selectively distributing these keys to the various users. By contrast, in this paper our work included an extended usage access control model and supports purpose hierarchy and granularity of data by using access purposes, purpose associated data models. We provided a rich variety of options that can deal with purpose data. Users can access purpose information with their keys at any time, even when their properties are updated. In our scheme, users have to satisfy pre-Authorizations, pre-Obligations and pre-Conditions as well as ongoing-Authorizations, ongoing-Obligations, ongoing-Conditions.

VI. Conclusions and Future Work

In this paper we presented a purpose-based access control suited for hierarchical data. We also proposed an efficient method for determining access purposes, which uses the notion purpose of subjects and objects by using usage control. Usage control models provide an approach for the next generation of access control. In usage control we analyse not only decision factors, such as authorizations, obligations and conditions, but also the continuity properties (Ongoing authorization). This paper also illustrates two different kinds of models built for purpose data. The methods presented in this paper can be used to control purpose data in a dynamic environment. It also begins a new application with usage control. This paper represents only a first step for authorization model in purpose data with usage control. Much work is still to be done before these models can be used in practice.

References

[1] Agrawal, R., Kiernan J., Srikant R. and Xu Y. (2002): Hippocratic databases. *Proc. 28th Int'l Conf. on Very Large Data Bases.* Hong Kong, China, 143-154.

[2] Bertion, E., Byun, J.-W. and Li, N. (2005): Privacy-preserving database systems. *Lecture Notes in Computer Science*. Springer Berlin, Heidelberg, 178-206.

[3] Bertion, E. and Ferrari E. (2002): Secure and selective dissemination of xml documents. *ACM trans, Inf. Syst. Secure*., 5(3):290-331.

[4] Bertion, E. and Sandhu, R. (2005): Database security-concepts, approaches, and challenges. *IEEE Transactions on Dependable and Secure Computing*. 02(1), 2-19.

[5] Byun, J.-W., Bertion, E. and Li, N. (2005): Purpose based access control of complex data for privacy protection. *'SACMAT'05: Proceedings of tenth ACM symposium on Access control models and technologies*. ACM. New York, NY, USA, 102-110.

[6] Byun, J.-W. and Li, N. (2004): Purpose-based access control for privacy protection in relational database systems. *Technical Report 2004-52*. Purdue University.

[7] Cao, J., Sun, L. and Wang, H. (2005): Towards secure xml documents with usage control. *Lecture Notes in Computer Science*. 3399, 296-307.

[8] Damiani, E., Paraboschi, S. and Samarati, P. (2002): A fine-grained access control system for xml documents. *ACM Trans. Inf. Syst. Secur.,* 5(2):169-202.

[9] Park, J. and Sandhu, R. (2002): Towards usage control models: beyond traditional access control. In *Proceedings of the seventh ACM symposium on Access control models and technologies*, page 57-64. ACM Press.

[10] Park, J., Sandhu, R., and Schifalacqua, J. (2003): Security architectures for controlled digital information dissemination. *In Proceedings of 16th Annual Computer Security Application Conference,* December 2003.

[11] Rabitti, F., Bertino, E., Kim, W. and Woelk, D. (1991): A model of authorization for next-generation database systems. In *ACM Transactions on Database Systems (TODS).*

[12] Sandhu, R. and Park, J. (2003): Usage control: A vision for next generation access control. In *MMM-ACNS 2003,* 17-31, Springer-Verlag Berlin Heideberg.

[13] Sun, L. and Li, Y. (2006): DTD level authorization in xml documents with usage control. In *International Journal of Science Network Security*, 244-250(6).

[14] Sun, L. and Li, Y. (2007): XML schems in xml documents with usage control. In *International Journal of Science Network Security*, 170-177(6).

[15] Sun, L. and Li, Y. (2008): Using usage control to access xml database, *International Journal of Information Systems in the Service Sector*, 32-44(1).

[16] Wang, H., Cao, J. and Zhang, Y. (2005): A flexible payment scheme and its role based access control. *IEEE Transactions on knowledge and Data Engineering*. 17(3), 425-436.

[17] Wang, H., Cao, J. and Zhang, Y. (2008): Access control management for ubiquitous computing. *Future Generation Computer Systems journal*. 870-878(24).

[18] Wang, H., Cao, J. and Zhang, Y. (2006): Ubiquitous computing environments and its usage access control, *Proceedings of the First International Conference on Scalable Information Systems.* ACM Press, Hong Kong, China, 72-81.

[19] World Wide Web Consortium (W3C). *Platform for Privacy Preferences (P3P)*. Available at www.w3.org.P3P.

[20] Zhang, X., Park, J. and Parisi-Presicce, F. (2004): A logical specification for usage control. In *SACMAT'4*. ACM Press.

[21] Zhang, X., Park, J. and Sandhu, R. (2003): Schema based xml security: Rbac approach. In *Proceedings of the IFIP WG*. ACM Press.

Lili Sun received her PhD degree in computer science from the University of Southern Queensland (USQ), Australia in 2010. She is currently a research assistant at the University of Southern Queensland. Her research interests include databases, Web service and access control for Electronic service system. She has published about 15 articles in international journals and conferences.

Hua Wang is an associate professor in the University of Southern Queensland. Dr Wang awarded a PhD degree in Computer Science from the University of Southern Queensland in 2004. He has been active in the areas of Information Systems Management, Distributed Database Management Systems, Access Control, Software Engineering and Electronic

Commerce. He has participated in research projects on mobile electronic system, Web service, and role-based access control for Electronic service system, and has already published over 100 research papers.
He is the co-editor-in-chief for ICST Transaction on Scalable Information Systems and was an editor of the special issue for International Journal of Security and Networks (IJSN) as well as an Editorial Board Member of The Open Cybernetics and Systemics Journal. He is also a member of the Australian Research Council Network in Enterprise Information Infrastructure.