Technical Note

Usage Control Model and Architecture for Data Confidentiality in a Database Service Provider

Amril Syalim,† Toshihiro Tabata†† and Kouichi Sakurai†††

A database service provider (DSP) is a provider of an Internet service for maintaining data so that users can access their data any time and anywhere via the Internet. The DSP model involves several challenges, including the issue of data confidentiality. In this paper we propose a Usage Control (UCON) model and architecture that can be enforced to support data confidentiality in the DSP model. Usage Control (UCON) is a unified model of access control that has been recently introduced as next generation access control. The basic idea of our UCON model for DSPs is separation of the control domain in a DSP into two parts: a database provider domain and a database user domain. In the database provider domain, the access control system controls access by users to database services. In the database user domain, the access control system controls access by other users to a user's database. Through this separation, we can define an access control policy for each domain independently.

1. Introduction

The Internet has changed the ways in which people communicate and interact with each other. Nowadays, many people use the Internet for sending email, reading news, finding jobs, and various other daily activities. It can also change the ways in which people and organizations manage their data. With rapid advances in networking and Internet technologies, it is possible to store data with an Internet provider to increase its availability.

A database service provider (DSP) is a provider of an Internet service for maintaining data so that users can access their data anywhere and any time via the Internet. DSP model offers at least two advantages to users. The first is that storing data with a DSP will increase the availability of the data [1], because the DSP is an online provider and users can access their data anywhere and any time via the Internet. The second advantage is that this model reduces the cost of the service, because the overall costs of the DSP can be amortized across a large number of users [3].

The DSP model also introduces several challenges. Besides issues concerning implementation technologies, there is also an issue as regards data confidentiality. Most users view their data as a valuable asset, so there is a need for sufficient security measures to guard the confidentiality of user data. In the DSP model, the provider should guarantee that user's sensitive data can only be accessed by authorized users. At the highest level of security, even the DSP itself should be guaranteed not to have access to the user's data.

In this paper, we propose an access control model and architecture that can be enforced to support data confidentiality in a DSP by developing a Usage Control (UCON) model and architecture for the DSP. The Usage Control (UCON) model is a unified model of access control that has recently been developed as a next-generation access control [7]. It extends the access matrix model, which has been used as an access control model for many years, by including support for trust management and digital rights management, which are required in modern applications. Trust management is supported by allowing authorization for a stranger's access based on credentials. Digital rights management is supported by including mutability of attributes, ongoing access control, and obligation-based access decisions. UCON also extends the access matrix model in its architecture. In the access matrix model, only a server-side reference monitor is required. The UCON architecture utilizes in addition to this, client-side reference monitor or both server-side and client-side reference monitors.

The basic idea of our UCON model for DSP is separation of the control domain in DSP into two parts: a database provider domain

† Graduate School of Information Science and Electrical Engineering, Kyushu University
†† Graduate School of Natural Science and Technology, Okayama University
††† Faculty of Information Science and Electrical Engineering, Kyushu University

and a database user domain. In the database provider domain, the access control system controls access by users to database services. In the database user domain, the access control system controls access by other users to a user's database. Through this separation we can define the access control policy for each domain independently.

The organization of this paper is as follows: Section 2 discusses the database service provider model. Section 3 discusses the core UCON ABC model and its architectures. Section 4 discusses the UCON model for data confidentiality in DSPs. Section 5 discusses the architecture of UCON for data confidentiality in DSPs. Section 6 concludes the paper.

2. Database Service Provider Model

The database service provider (DSP) model is an implementation of a new business model where people and organizations want to store their data on the Internet to increase its availability. The DSP model is shown in **Fig. 1**.

As illustrated in Fig. 1, in the DSP model, users store their data on a DSP server and can access their data via the Internet. Since in the DSP model the users' data resides on the DSP server, the service provider needs to provide sufficient security measures to protect the confidentiality of this data.

In this paper, we present an access control model and architecture that can be enforced in a DSP to support data confidentiality of the DSP's users. The idea of our access control model is shown in **Fig. 2**. We separate domain control in a DSP into two domains: the database provider domain and the database user domain. In the database provider domain, the access control system controls access by users to database services. In the database user domain, the access control system controls access by other users to a user's database. Through this separation we can guarantee the confidentiality of users' data because even the DSP itself does not have control over the users' databases. We give details of the model in Section 4 and Section 5.

3. Usage Control

Usage Control (UCON) is a unified model of traditional and modern access controls. The core model of UCON is the ABC Model, which consists of eight components: subjects, objects, subject attributes, object attributes, rights, authorization, obligations, and conditions [5] (see **Fig. 3**).

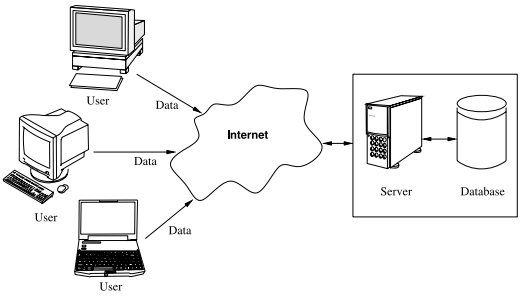

Fig. 1 Database service provider model.

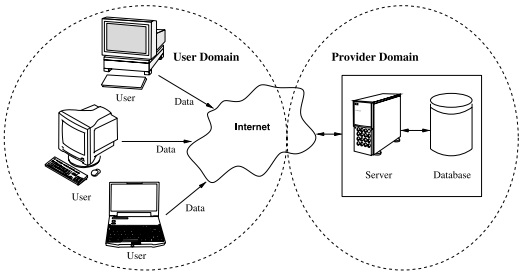

Fig. 2 Domain separation in DSP.

Subjects and objects are active and protected entities in the system. Rights are privileges of a subject with respect to an object. The concept of subjects, objects and rights in UCON is borrowed from that of subjects, objects, and rights in the traditional access matrix model. Subject attributes and object attributes are properties that can be used during a decision process. In the Usage Control ABC model, subject and object attributes can be mutable as a consequence of access. This property is called mutability of attributes. An immutable attributes can be changed only by administrative action.

Authorizations, obligations, and conditions are three usage decision factors in the UCON model. Authorizations are decision factors based on subject and object attributes. They are usually required prior to access, but in addition it is possible to require ongoing authorizations during access. Authorizations may require updates for subject and/or object attributes. These updates can be made either before, during, or after access. Ongoing authorization (during access) is another property of UCON, called continuity of decision, that can also be applied to obligations based usage decision factors.

Obligations are requirements that a subject must perform before (pre-) or during access

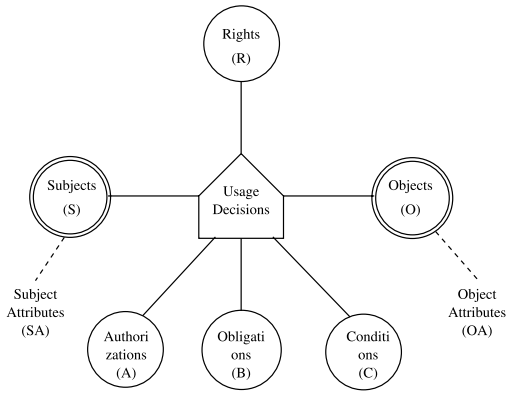

Fig. 3 Usage Control ABC Model.

Table 1 The 16 basic UCON models.

	0(im-mutable)	1(pre-update)	2(ongoing-update)	3(post-update)
preA	Y	Y	N	Y
onA	Y	Y	Y	Y
preB	Y	Y	N	Y
onB	Y	Y	Y	Y
preC	Y	N	N	N
onC	Y	N	N	N

preA: pre- Authorizations
onA: ongoing Authorizations
preB: pre- Obligations
onB: ongoing Obligations
preC: pre- Conditions
onC: ongoing Conditions

(ongoing). Subject and/or object attributes can be used to decide what kind of obligations are required for access approval. The exercise of obligations may update mutable attributes. These updates can affect current or future usage decisions. Conditions are environmental or system-oriented decision factors. Conditions are not under the direct control of individual subjects. Evaluation of conditions cannot update any subject or object attributes.

On the basis of these three decision factors, continuity and mutability properties, there are 16 possible basic models of UCON [7]. Access control models in the real world can utilize more than one of these basic models, which are shown in **Table 1**.

The architecture of UCON, based on the structure of reference monitors, extends the access matrix model by utilizing not only a server-side reference monitor (SRM), but also a client-side reference monitor (CRM) or both server-side and client-side reference monitors [6]. An SRM controls a subject's access to and usage of objects by means of a reference monitor exists in the server-side system. A subject can be either within the same organization/network area or outside the area (see **Fig. 4**). A control domain is an area of coverage where the rights and usage of rights to objects are under the control of the reference monitor.

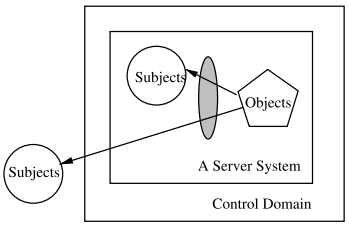

Fig. 4 Control domain with SRM.

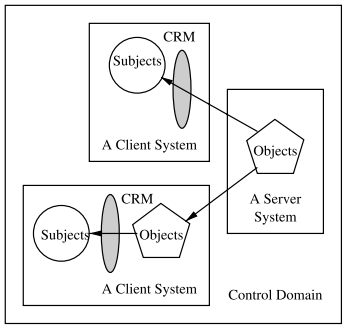

Fig. 5 Control domain with CRM.

In a CRM environment, no reference monitor exists in the server-side system. Instead, a reference monitor exists in the client system to control usage of objects. In this environment objects can be stored either centrally or locally. Since there is a CRM, the usage of objects saved on the client side is under the control of the CRM rather than the server (see **Fig. 5**) [6].

4. Usage Control Model for Data Confidentiality in a Database Service Provider

In this section, we discuss the UCON model for a DSP. The basic idea of the UCON model is to separate the control domain in a DSP into two parts: a database provider (DP) domain and a database user (DU) domain (see **Fig. 6**). In the database provider domain, access control system controls access from users to database services. In the database user domain, the access control system controls access by other users to a user's database. Through this separation, we can define an access control policy for each domain independently.

4.1 UCON Model for the Database Provider Domain

The access control system in the database

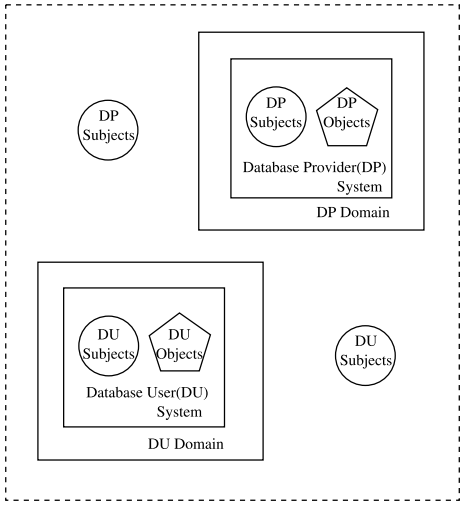

Fig. 6 Domain separation in DSP.

provider domain controls access by users in DSP to database services. Users in DSP are registered to use database services provided by the DSP in order to store their data. The access control system in this domain is administered by the DSP administrator. The DSP administrator can freely define an access control policy for this domain without compromising the confidentiality of user data.

As an example, we show two policies that can be defined by DSP administrator. In Example 4.1, the administrator defines a DAC (discretionary access control) policy for the DSP using $UCON_{preA_0}$(the UCON model with pre-authorization decision and immutable attributes – see Table 1). In Example 4.2, the administrator defines a policy for the DSP whereby a user has to pay for the use of database services on the basis of the length of access time (in minutes), using $UCON_{preA_3}$ (the UCON model with pre-authorization decision and post-update attributes).

Example 4.1. DAC policy in the database provider domain using $UCON_{preA_0}$:

S is a set of users
O is a set of database services
R is a set of rights
$ATT(S)$ is a set of attributes of S
$ATT(O)$ is set of attributes of O
allowed is a usage decision function that allows a user to access a database service o with right r

N is a set of identity names
$id : S \rightarrow N$, one-to-one mapping
$ACL : O \rightarrow 2^{N \times R}$
$ATT(S) = id$
$ATT(O) = ACL$

$allowed(s, o, r) \Rightarrow (id(s), r) \in ACL(o)$

Example 4.2. Service usage policy in the database provider domain using $UCON_{preA_3}$:

S is a set of users
O is a set of database services
R is a set of rights
$ATT(S)$ is a set of attributes of S
$ATT(O)$ is set of attributes of O
allowed is a usage decision function that allows a user to access a database service o with right r

M is a set of money amounts
ID is a set of membership
$TIME$ is the current usage in minutes
$member : S \rightarrow ID$
$expense : S \rightarrow M$
$usageT : S \rightarrow TIME$
$value : O \times R \rightarrow M$ (the cost per minute of r on o)
$ATT(s) : member, expense, usageT$
$ATT(o, r) : valuePerMinute$

$allowed(s, o, r) \Rightarrow member(s) \neq \oslash$
$postUpdate(expense(s)) : expense(s) = expense(s) + (value(o, r) \times usageT(s))$

4.2 UCON Model for Database User Domain

In the database user domain, the access control system controls access by other users to a user's database. The other users are not necessarily also registered users in the DSP (users that have access to database services in the DSP). Access in this domain is controlled by the user who owns the database. The user can freely define an access control policy for the domain.

As an example, we show two policies that can be defined by the user in order to control access to his or her database. In Example 4.3, the user defines an RBAC (role-based access control) policy in his or her database, using $UCON_{preA_0}$. In Example 4.4, the user utilizes trust management using $UCON_{preA_0}$.

Example 4.3. RBAC policy in the database user domain using $UCON_{preA_0}$:

S is a set of other users
O is a set of database tables
R is a set of rights
$ATT(S)$ is a set of attributes of S
$ATT(O)$ is set of attributes of O
allowed is a usage decision function that allows other users to access a database table o with right r

$P = (o, r)$
$ROLE$ is a partially ordered set of roles with dominance relation $\geq$
$actRole : S \rightarrow 2^{ROLE}$
$Prole : P \rightarrow 2^{ROLE}$
$ATT(S) = actRole$
$ATT(O) = Prole$
$allowed(s, o, r) \Rightarrow \exists role \in actRole(s), \exists role' \in Prole(o, r), role \geq role'$

Example 4.4. A user utilizes trust management in the database user domain using $UCON_{preA_0}$:

S is a set of other users
O is a set of database tables
R is a set of rights
$ATT(S)$ is a set of attributes of S
$ATT(O)$ is set of attributes of O
allowed is a usage decision function that allows other users to access a database table o with right r

$GROUP$ is a set of group names
$cert : S \rightarrow 2^{GROUP}$
$ATT(s) : cert$
$ATT(o) : groupID$

$allowed(s, o, r) \Rightarrow (cert(s) \neq \oslash) \wedge groupID(o) \in cert(s)$

5. Usage Control Architecture for Data Confidentiality in a Database Service Provider

The architecture of the UCON model discussed in Section 4 is illustrated in **Fig. 7**. There are two control domains: the database provider (DP) domain and the database user (DU) domain. In the database provider domain, the access control system restricts access by users of a DSP to database services. In the database user domain, the access control system controls access by other users to a user database.

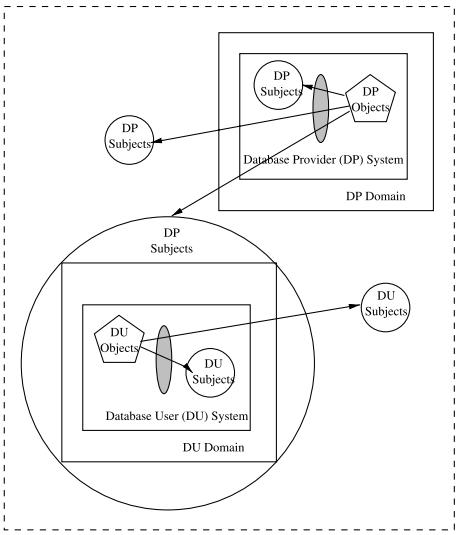

Fig. 7 Architecture of the UCON model for data confidentiality in DSP.

As shown in Fig. 7, a database user system that controls access in the database user domain is also a subject of the database provider domain. Although, to provide access to objects in its domain, the database user system needs to access objects in the database provider domain, the database provider system that controls access to objects in the database provider domain does not have control over the objects in the database user domain.

The database provider system and the database user system utilize the server-side reference monitor (SRM) to control access to objects in their domains.

6. Conclusion

In this paper, we have proposed an access control model and an architecture that can be enforced in a database service provider (DSP) by developing a Usage Control (UCON) model and architecture of the DSP. The basic idea of the UCON model is separation of the control domain in a DSP into two parts: a database provider domain and a database user domain. In the database provider domain, the access control system controls access by users to database services. In the database user domain, the access control system controls access by other users to a user's database. Through this separation we can define an access control policy for each domain independently.

References

1) Bouganim, L. and Pucheral, P.: Chip-Secured Data Access: Confidential Data on Untrusted Servers, *Proc. 28th Very Large Data Bases Conference*, Hongkong, China (2002).
2) Damiani, E., De Capitani di Vimercati, S., Jajodia, S., Paraboschi, S. and Samarati, P.: Balancing Confidentiality and Efficiency in Untrusted Relational DBMSs, *CCS'03*, Washington, DC, USA (2003).
3) Hacigümüş, H., Iyer, B., Li, C. and Mehrotra, S.: Executing SQL over Encrypted Data in the Database-Server-Provider Model, *Proc. ACM SIGMOD Conference*, Madison, Wisconsin, USA (2002).
4) Kantarcioğlu, M. and Clifton, C.: Security Issues in Querying Encrypted Data, Purdue Computer Science Technical Report 04-013, Purdue University (2004).
5) Park, J. and Sandhu, R.: The UCON_{ABC} Usage Control Model, *ACM Trans. Inf. Syst. Security*, Vol.7, No.1, pp.128–178 (Feb. 2004).
6) Park, J. and Sandhu, R.: Toward Usage Control Models: Beyond Traditional Access Control, *SACMAT '02*, Monterey, California, USA (2002).
7) Sandhu, R. and Park, J.: Usage Control: A Vision for Next Generation Access Control. *The Second International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security* (*MMM-ACNS*), St. Petersburg, Rusia (2003).

(Received August 29, 2005)
(Accepted November 1, 2005)
(Online version of this article can be found in the IPSJ Digital Courier, Vol.2, pp.39–44.)

Amril Syalim received B.Sc. degree in computer science from Faculty of Computer Science, University of Indonesia in 2003. He is currently working toward the M.E. degree in the Graduate School of Information Science and Electrical Engineering, Kyushu University. His current research interests are in the area of access controls and database security.

Toshihiro Tabata received the B.E. degree in 1998, the M.E. degree in 2000, and the Ph.D. degree in engineering in 2002, all from the Kyushu University, Fukuoka, Japan. He had been a research associate of Information Science and Electrical Engineering at Kyushu University since 2002. He has been an associate professor of Graduate School of Natural Science and Technology, Okayama University since 2005. His interests include operating system and computer security. He is a member of the Information Processing Society of Japan (IPSJ), IEICE, ACM and USENIX.

Kouichi Sakurai received the B.S. degree in mathematics from Faculty of Science, Kyushu University and the M.S. degree in applied science from Faculty of Engineering, Kyushu University in 1986 and 1988, respectively. He had been engaged in the research and development on cryptography and information security at Computer and Information Systems Laboratory at Mitsubishi Electric Corporation from 1988 to 1994. He received the Dr. degree in engineering from Faculty of Engineering, Kyushu University in 1993. Since 1994 he has been working for Department of Computer Science of Kyushu University as an associate professor, and now he is a full professor from 2002. His current research interests are in cryptography and information security. Dr. Sakurai is member of the Information Processing Society of Japan, ACM and the International Association for Cryptologic Research.