A Role-involved Conditional Purpose-based Access Control Model

Md. Enamul Kabir, Hua Wang, Elisa Bertino

A Role-involved Conditional Purpose-based Access Control Model

Md. Enamul Kabir[1], Hua Wang[1] and Elisa Bertino[2]

[1]Department of Mathematics & Computing
University of Southern Queensland
Toowoomba, QLD 4350, Australia
{kabir,wang}@usq.edu.au
[2]Department of Computer Science and CERIAS
Purdue University, West Lafayette, Indiana, USA
bertino@cs.purdue.edu

Abstract. This paper presents a role-involved conditional purpose-based access control (RCPBAC) model, where a purpose is defined as the intension of data accesses or usages. RCPBAC allows users using some data for certain purpose with conditions. The structure of RCPBAC model is defined and investigated. An algorithm is developed to achieve the compliance computation between access purposes (related to data access) and intended purposes (related to data objects) and is illustrated with role-based access control (RBAC) to support RCPBAC. According to this model, more information from data providers can be extracted while at the same time assuring privacy that maximizes the usability of consumers' data. It extends traditional access control models to a further coverage of privacy preserving in data mining environment as RBAC is one of the most popular approach towards access control to achieve database security and available in database management systems. The structure helps enterprises to circulate clear privacy promise, to collect and manage user preferences and consent.

Key words: Access control, Conditional Purpose, Privacy.

1 Introduction

Nowadays privacy becomes a major concern for both consumers and enterprises and thus privacy preservation is a challenging problem. Enterprises collect customer's private information along with other attributes during any kind of marketing activities. It is a natural expectation that the enterprise will use this information for various purposes, this leading to concerns that the personal data may be misused. As individuals are more concerned about their privacy, they are becoming more reluctant to carry out their businesses and transactions online, and many organizations are losing a considerable amount of potential profits [9]. Therefore without a clear compromising between individuals and enterprises, data quality and data privacy cannot be achieved and so many organizations are

seriously thinking about privacy issues of consumers. By demonstrating good privacy practices, many businesses are now trying to build up solid trust to customers, thereby attracting more customers [4]. Considering the privacy of customers, enterprise has to develop a secure privacy policy to remove the fear of customers. Thus in an internal management system, a reliable, efficient, effective and secure privacy policy should be established depending on customer's requirements.

One of the most popular approach for protecting private information is the access control model. Access control is the process of limiting access to the resources of a system only to authorized users, programs, processes, or other systems [23]. The traditional access control model focus on which user is performing which action on which data objects and completely ignores which purpose data will be used. It also overlook to take consent from customers of using their private data. Thus it can be said that personal information can be collected, stored and used without any consent of customers that make them fear of breaching privacy. So the access control model should be developed in such a way that satisfy customer requirement as well as specify which purpose data will be used for. Observing the lack of adequate privacy protecting systems, Byun *et al.* [7] proposed a privacy preserving access control model for relational databases based on the notion of purpose following an idea of Agrawal [1].They argue that the notion of purpose must play a major role in access control models and that an appropriate metadata model must be developed to support such privacy centric access control models in order to protect data privacy. An approach is developed that is based on intended purposes and access purposes corresponding to the data object and the data access respectively which makes access control clearer. Usually, during the data collection procedure customers are informed about the purposes of enterprises. Customers then decide whether their information could be used or not for a certain purpose. That means data providers are given an option of using their data with certain purposes. If an individual mentions that his/her data could not be used for a certain purpose, then his/her information is not accessible for the purpose. Generally data providers are reluctant to use any part of their information for any purposes and so there is a possibility of losing information. But more information can be extracted from data providers by providing more options of using their information. An intended purpose is divided (IP) into two parts: Allowed Intended Purposes (AIP) (explicitly allows to access the data for the particular purpose) and Prohibited Intended Purpose (PIP) (data access for particular purposes are never allowed). In our previous work [11], we included another term conditional intended purpose (CIP) (Conditionally allows to access the data for the particular purpose) to extract information from PIP, which referred to conditional purpose-based access control (CPBAC) model. The key characteristics of CPBAC model was that it allows users using some data with certain conditions and multiple purposes can be associated with each data element. Our previous work exploited query modification techniques to support data access control based on the conditional purpose information. However, RBAC is one of the most popular approach towards access

control to achieve database security and available in many database management system, need to address it in CPBAC. To implement this, we need to expand CPBAC model with the conventional well-known RBAC. Such an extension of CPBAC with roles which we refer to role-involved conditional purpose-based access control (RCPBAC) model is presented in this paper. Both access purposes and intended purposes are specified with respect to a hierarchical structure that organizes a set of purposes for a given enterprise.

Role based access control (RBAC) proposed by Sandhu *et al.* [18] has been widely used in database system management and operating system products because of its significant impact on access control systems. RBAC is described in terms of individual users being associated with roles as well as roles being associated with permissions (each permission is a pair of objects and operations). As such, a role is associated with users and permissions. A user in this model is a human being and a role is a job function or job title within the organization associated with its authority and responsibility. RBAC model also includes a role hierarchy, a partial order defining a relationship between roles, to facilitate the administration tasks. In this paper we utilize RBAC which supports conditional purpose into our model. Thus RCPBAC model has the following features:

- It satisfies data providers requirements and allows users using data with conditions. The data provider express his/her own privacy preferences through setting intended purpose with three levels (AIP, CIP and PIP), while the data owner is responsible for working out the policies for authorization of access purpose.
- Its algorithm utilizes RBAC to achieve the compliance computation between access purpose and intended purpose.
- It extracts more information from data providers by providing more possible options of using their information assuring privacy of private information that maximizes the usability of data.
- It determines the compliance computation between access purpose and intended purpose. Intended purposes are associated with the requested data objects during the access decision to the well-designed hierarchy of private metadata.

The reminder of this paper is organized as follows. We present a brief overview of privacy related technologies in Section 2. Since purpose is used as the basis of access control, a brief description of the notion of purpose is described in Section 3. In Section 4 we present comprehensive descriptions of our proposed access control model with roles. Access decision of the proposed RCPBAC model is illustrated in Section 5. Concluding remarks are included in Section 6.

2 Related Work

This work is related to several topics in the area of privacy preservation in data mining atmosphere. The most notable technique to protect privacy is the W3C's Platform for Privacy Preferences (P3P) that formally specify privacy policy by

service providers [13]. Byun *et al.* [7] indicate that P3P does not provide any functionality to keep promises in the internal privacy practice of enterprise. Thus it can be said that a striking privacy policy with inadequate enforcement mechanism may place the organizations at risk of reputation damage. The concept of Hippocratic database introduced by Agrawal *et al.* [1] that amalgamates privacy protection in relational database system. A Hippocratic database includes privacy policies and authorizations that associate with each attribute and each user the usage purpose(s) [3]. Agrawal *et al.* [1] presented a privacy preserving database architecture called Strawman which was based the access control on the notion of purposes, and opened up database-level researchers of privacy protection technologies. After that, purpose based access control introduced by Byun *et al.* [6, 7] and Yang *et al.* [21], fine grained access control introduced by Agrawal *et al.* [2] and Rizvi *et al.* [15] are widely used access control models for privacy protection. In IT system the proposed Enterprise Privacy Authorization Language (EPAL) of IBM [10] is a language for writing enterprise privacy policies to run data handling practices.

A lot of works [5, 8, 16, 17, 19] provide many valuable insights for designing a fine-grained secure data model. In a multilevel relational database system, every piece of information is classified into a security level, and every user is assigned a security clearance [7]. LeFevre *et al.* [12] proposed an approach to enforcing privacy policy in database setting. This work focus on ensuring limited data disclosure, based on the premise that data providers have control over who is allowed to see their personal data and for what purpose. Peng *et al.* [22] proposed an approach for privacy protection based on RBAC. The key feature of their approach is dynamic and they proposed Dynamic purpose-based access control. This method however works based on subject attribute and system attribute but does not guarantee to extract more information. Byun *et al.* [7] present a comprehensive approach for privacy preserving access control model. In their access control model multiple purposes to be associated with each data elements and also support explicit prohibitions. Massacci *et al.* [14] also mention that most privacy-aware technologies use purpose as a central concept around which privacy protection is built.

All of these works proposed different approaches to protect the privacy of individuals through different models without being considering to extract more information. Our aim is to preserve privacy of individuals as well as extracting more information. With this aim, this paper investigated RBAC to extend our previous work on CPBAC [11]. It has improved in four different ways. First, we introduce conditional purpose in the intended purpose in addition to explicit prohibitions that make data providers more flexible to give information. Second, the enterprise can publish an ideal privacy policy to manage data in a sensitive, effective and trustworthy way. Third, it reduces the information loss as it shows that we can extract more information from data providers and fourth it can easily be implemented in RBAC, where a RBAC model has made a significant impact on many access control systems.

3 Purpose, Access Purpose and Intended Purpose

Data is collected for certain purpose. Each data access also serves a certain purpose. Thus a privacy policy should concern which data object is used for which purposes.

Purpose
Purpose is the most important thing to researchers as it directly shows how access to data elements has to be controlled. P3P defines purpose as "the reason(s) for data collection and use" and specifies a set of purposes [20]. In commercial surroundings purposes normally have a hierarchical associations among them; i.e., generalization and specialization relationships. We borrow the purpose definition from [7].

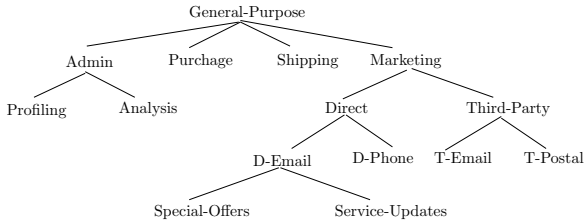

Fig. 1. Purpose Tree

Definition 1: (Purpose and Purpose Tree): A purpose describes the intentions for data collection and data access. A set of purposes, denoted as ω, is organized in a tree structure, referred to as Purpose Tree and denoted as Ω, where each node represents a purpose in ω and each edge represents a hierarchical relation between two purposes. Figure 1 is an example of purpose tree. Purposes, depending on their association with objects and subjects, may be called intended purposes or access purposes respectively.

Definition 2 (Access Purpose): An access purpose is intensions for accessing data objects, and it must be determined by system when data access is requested. So access purpose specifies the purpose for which a given data element is accessed.

Definition 3 (Intended Purpose): An intended purpose is the specified usages for which data objects are collected. That is, purpose associated with data and thus regulating data accesses as intended purpose. According to our approach an intended purpose consists of the following three components.

Allowable Intended Purpose (AIP): This means that data providers explicitly allow accessing the data for a particular purpose. For example data providers may consider that his/her information can be used for marketing purpose without any further restrictions.

Conditional Intended Purpose (CIP): This means that data providers allow accessing the data for a particular purpose with some conditions. For example

data providers may consider that his/her income information can be used for marketing purpose through generalization.

Prohibited Intended Purpose (PIP): This means that data providers strictly disallow accessing the data for a particular purpose. For example data providers may consider that his/her income information cannot be used for marketing purpose. In that case data provider's income attribute is strictly prohibited to use for marketing purpose. Notice that each data element is stored in three different purposes each of which corresponds to a particular intended purposes.

So an intended purpose IP is a tuple $\langle AIP, CIP, PIP\rangle$, where AIP $\subseteq \omega$, CIP$\subseteq \omega$ and PIP$\subseteq \omega$ are three sets of purposes. The set of purposes implied by IP, denoted by IP* and the set of conditional purposes, denoted by IP$^\star_c$ are defined to be AIP$^\downarrow$-CIP$^\updownarrow$-PIP$^\updownarrow$ and CIP$^\downarrow$ -PIP$^\updownarrow$ respectively, where

R$^\downarrow$, is the set of all nodes that are descendants of nodes in R, including nodes in R themselves,

R$^\uparrow$, is the set of all nodes that are ancestors of nodes in R, including nodes in R themselves, and

R$^\updownarrow$, is the set of all nodes that are either ancestors or descendants of nodes in R, that is, R$^\updownarrow$=R$^\uparrow \cup$ R$^\downarrow$.

Definition 4 (Full Access Purpose Compliance): Let Ω be a purpose tree. Let IP= $\langle AIP, CIP, PIP\rangle$ and AP be an intended purpose and an access purpose defined over Ω, respectively. AP is said to be compliant with IP according to Ω, denoted as AP$_{\Leftarrow\Omega}$IP, if and only if AP$\in$ IP*.

Definition 5 (Conditional Access Purpose Compliance): Let Ω be a purpose tree. Let IP= $\langle AIP, CIP, PIP\rangle$ and AP be an intended purpose and an access purpose defined over Ω, respectively. AP is said to be conditionally compliant with IP according to Ω, denoted as AP$_{c\Leftarrow\Omega}$IP, if and only if AP$\in$ IP$^\star_c$.

Example 1: Suppose IP= $\langle$\{Admin, Direct\}, \{Third-party\}, \{D-mail\}$\rangle$, then IP* = \{Admin, Profiling, Analysis, D-Phone\} and IP$^\star_c$ = \{Third-party, T-Email, T-Postal\}, where subscript c indicates that customers information can be used for the purpose with some conditions.

4 Conditional Purpose-based Access Control (CPBAC)

In the CPBAC model data providers are asked three possible options for usage of each data item. Permissible usage means data providers allow to use of their data, prohibited means data providers don't allow to use their data and conditional permissible usages means data providers conditionally allow to use of their data item. Consider Table 1 that describes the intended purpose, types of data and possible data usages. For example, a data provider may select his/her name is permissible for **Admin** purpose, address is not permissible for **Shipping** purpose but income information is conditionally permissible for **Marketing** purpose. That is, data provider does not have any privacy concern over the name when it is used for the purpose of administration, great concern about privacy of the address information (and so does not want to disclose address) when it is used for the purpose of shipping, but his/her income information can be used for

Table 1. Intended purpose, data type and data usage type

Term	Description	Example
Intended Purpose	Intended usage of data specified by data provider	AIP, CIP, PIP
Data item	Types of data being collected (i.e. attributes)	Name, Age, Income
Data usage Type	Types of potential data usage (i.e. purpose)	Marketing, Admin

marketing purpose with some conditions. Here the term "conditions" means that data providers ready to release his/her certain information for certain purpose by removing his/her name or id or through generalization. This information is then stored in the database along with the collected data, and access to the data is tightly governed according to the data provider's requirements. For using the term condition data providers feel more comfortable to release their data. Table 2 shows conditional records and intended purposes of a data provider Alice. The design of intended purposes supports permissive, conditions and prohibitive

Table 2. Conditional records and intended purposes

	name	age	address	income
AIP	Alice	35	21, West St., TBA, QLD 4350	35000
CIP	A	30-40	West St., TBA, QLD 4350	30000-40000
PIP	$\star$	$\star$	$\star$	$\star$

$\star$ means data providers are reluctant of any usage of their data items

privacy policies. This construction allows more squash and flexible policies in our model. Moreover, by using CIP and PIP, we can assure that data access for particular purposes are allowed with some conditions or never allowed. Note that an access decision is made based on the relationship between the access purpose and the intended purpose of the data. Access is allowed only if the access purpose is included in the implementation of the intended purpose; in that case the access purpose is compliant with the intended purpose. The access is accepted with conditions if the implementation of intended purpose includes the access purpose with conditions; in this case we say that access purpose is conditionally complaint with intended purpose. The access is denied if the implementation of the intended purpose does not include the access purpose, in this case access purpose is not complaint with the intended purpose.

4.1 Role-involved CPBAC (RCPBAC)

RBAC model is a landmark in the field of access control models and become a NIST standard [18]. The key concept of RBAC model is role which represents

certain job function or job title within the organization. The permission of performing certain operations on certain data is assigned to roles instead of to single users. Users are thus simply authorized to play the appropriate roles, thereby acquiring the roles authorizations. When the user makes a request, the system activates specific roles predefined for him/her. Thus he/she gains the permission of operating directly or indirectly from roles, which considerably simplifies the authorization management. Because roles represent organizational functions, an RBAC model can directly support security policies of the organization. In the recent development of privacy preserving data mining environment many researchers have been confessed the importance of purpose, but in the RBAC model purpose is not yet fully investigated. Based on RBAC, CPBAC model extends mainly in the following aspects.

- The access permission is no longer a 2-tuple $\langle Object, Operation \rangle$, but a 3-tuple $\langle Object, Operation, AccessPurpose \rangle$ which is called the access purpose permission.
- The access purpose permission is assigned to roles and after the purpose compliance process, only the objects which are purpose compliant or conditionally compliant can be returned to the users.

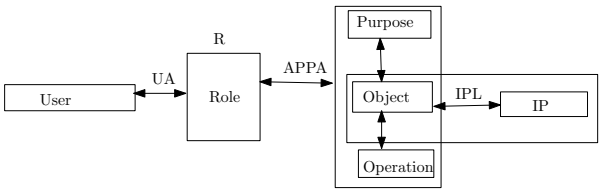

Fig. 2. RCPBAC Model

In RCPBAC model, the entity User is defined as a human being, a machine, a process, or an intelligent autonomous agent, etc. The entity Role represents the working function or working title assigned within the organization according to different authorities and obligations. Roles are created for the various job functions in an organization and users are assigned roles based on their authority and qualifications. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated and permission can be revoked from roles as needed. The entity Object stands for the data which the user requests and can be abstracted as data set. The entity operation signifies certain action that the user wants to perform on the object. The entity Purpose represents all the possible access purposes in the system and IP signifies the intended purposes with three levels (AIP, CIP, PIP) attached with each data object. Permission is an approval of a particular operation to be performed on one or more objects. The RCPBAC model is illustrated in Figure 2. The formalized definition of RCPBAC model is shown as follows:

Definition 6 (RCPBAC model):

- *User, Role, Operation, Object, Purpose* represent the set of users, roles, operations, objects and purposes.
- IP=$\{\langle aip, cip, pip\rangle | aip \subseteq \omega, cip \subseteq \omega, pip \subseteq \omega\}$ is the set of object's intended purposes, where *aip* signifies the object's permitted intended purpose, *cip* is the conditionally permitted intended purpose and *pip* represents the object's forbidden intended purposes [11].
- R=$\{r | r \in Role\}$ is the set of roles.
- APP=$\{\langle o, opt, ap\rangle | o \in Object, opt \in Operation, ap \in Purpose\}$ is the set of access purpose permissions.
- IPL=$\{\langle o, ip\rangle | o \in Object, ip \in IP\}$ represents the set of data objects and their predefined intended purpose.
- $RH \subseteq Role \times Role$ is a partial order on roles, called the inheritance relationship among roles. We also define a partial order $\geq$ which is the transitive closure of RH. For example, $r_1 \leq r_2$ means r_1 inherits all permissions of r_2. Figure 3 is an example of role hierarchies of Marketing department for a hypothetical company.
- $PT \subseteq Purpose \times Purpose$ is a partial order on purposes (generalization/ specialization) shown in the purpose tree. Figure 1 is an example of purpose tree.
- *User Assignment* $UA \subseteq User \times Role$ is a many-to-many mapping relation between users and their assigned roles.
- *Access Purpose Permission Assignment* $APPA \subseteq Role \times APP$ is a many-to-many mapping relation between roles and access purpose permissions. It signifies the action that certain role performs on certain object on certain access purpose.
- *Purpose Compliance* $PC \subseteq APP \bowtie IPL$ ia a one-to-one relation between each access purpose permission and data object as well as its predefined intended purposes.

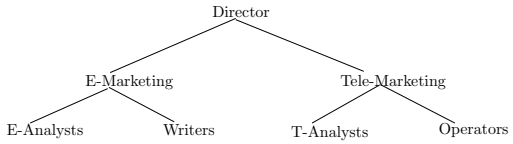

Fig. 3. Example of Role Hierarchies

Now we are at the stage to provide function definitions to facilitate the discussion of RCPBAC model.

- $assigned\_role : User \rightarrow 2^{Role}$, the mapping of a user u onto a set of roles. Formally,
  $assigned\_role(u) = \{r \in Role | \langle u, r\rangle \in UA\}$

- $assigned\_access\_purpose\_permission$: $Role \rightarrow 2^{APP}$, the mapping of a role r onto access purpose permissions. Formally,
  $assigned\_access\_purpose\_permission(r) = \{app \in APP | \langle app, r\rangle \in APPA\}$
- $Purpose\_binding$: $Object \rightarrow IP$, the mapping of a data object o onto intended purposes ip with three levels, which means finding the bound intended purposes of the object.
- $Purpose\_compliance$: $AP \times IP \rightarrow \{True, Conditionally\,True, False\}$, is used to determine the compliance between the access purpose and the object's intended purposes [11]. Formally,
  $Purpose\_compliance(ap, ip)$=True iff $ap \in IP^{\star}$,
  $Purpose\_compliance(ap, ip)$=Conditionally True iff $ap \in IP_c^{\star}$.

In RCPBAC model, the users are required to explicitly state their access purpose(s) when they try to access data. That is, the users present an access purpose for each query they issue. During the access decision process, the system combines the requested data with its intended purposes according to privacy metadata and sends the data whose intended purposes are fully compliant or conditionally compliant with the access purpose to the requester. As the model respects customers requirement regarding their data usages and also support RBAC, it prevents private information from disclosure.

4.2 Authorization and Authentication

Access purpose is the reason for accessing a data item and it must be determined by the system when a data access is requested. There are different possible methods for determining the access purpose [7]. Among the various possible techniques to determine access purpose, in this paper we utilize the method where the users are required to explicitly state their access purposes when they try to access data. In the RCPBAC model, access purposes are authorized to users through roles. Users are required to state their access purposes along with their queries and the system confirms the stated access purposes by ensuring that the users are indeed allowed to access data for the particular purposes. Now we formally define access purpose authorization and its authentication.

Definition 7 (Access Purpose Authorization) Let Ω be a purpose tree and ω be the set of purposes in Ω. Also let R be the set of roles defined in a system. An access purpose is authorized to a specific set of users by a pair $\langle ap, r\rangle$, where ap is a access purpose in ω and r is a role defined over R.

Usually in the typical situation, roles and access purpose are organized in a hierarchical structure. All users authorized for a role r_i are also authorized for any role r_j where $r_i \geq r_j$. Thus, activating a role r_i automatically activates all roles r_j, such that $r_i \geq r_j$. Similarly, authorizing an access purpose ap for a role r_i implies that the users belonging to r_i (or the users belonging to r_j, where $r_i \geq r_j$) are authorized to access data with ap as well as all the descendants of ap in the purpose tree. The access purpose authentication definition below confines the implications of access purpose authorizations.

Definition 8 (Access Purpose Authentication): Let Ω be a purpose tree, ω be the set of purposes in Ω and R be the set of roles defined in a system. Suppose that an access purpose ap and a role r_i activated by a user u. We say that ap is legitimate for u under r_i if there exists an access purpose authorization $\langle ap_l, r_i \rangle$, where ap_l in ω and r_i is a role defined over R such that $ap \in$ Descendants (ap_l) and the users belongs to role r_i (or any descendants role of r_i.)

Consider the purpose tree in Figure 1 and the role hierarchies of Marketing department for a hypothetical company in Figure 3. Suppose that access purpose "Service-Updates" are assigned to the "E-Marketing" role. Then the users who activate the role "E-Marketing" (or the two descendants role) can access data for the purpose of "Service-Updates".

Table 3. Intended purposes table

Sl_No.	Table_ID	Table_Name	Cus_ID	Attr_Name	Intended_Purpose
1	1	Customer_info	22	Customer_Name	⟨{General}, {Admin}, {Shipping}⟩
2	1	Customer_info	25	Income	⟨{Marketing}, {Admin}, {Shipping}⟩
3	1	Customer_info	52	Address	⟨{Shipping}, {Admin}, {Marketing}⟩

By access purpose authorization and authentication, users get access purpose permission from access control engine. Now it is necessary to check whether users access purpose is fully or conditionally compliant with data's intended purpose for access decision. In the following Section we discuss the compliance computation for access decision.

5 Access Decision

In our model customers are given three more possible options of using their data. These make them comfortable to release their data fully or conditionally and the private information will be protected. After data are collected, intended purposes with three different levels will be associated with data. As intended purpose is assigned to every data element, an intended purposes table (IPT) is formed. Consider a typical IPT table in Table 3 which consists of six columns, where Sl_No is the serial number, Table_ID is the identification of the original table, Cus_ID is the hidden attribute which is added when tables are created, Table_Name is the name of the table in the database and Attr_Name is the attribute name in the table. Thus the storage of intended purposes and data are separated. Data providers (customers) are able to control the release of their data by adding privacy levels into the IPT which will not affect data in the database. After authorizing access purpose, users get access purpose permission

Table 4. Compliance computation and access decision algorithm

Comp_Check$_1$ (ap, $\langle AIP, PIP\rangle$)
/⋆ This function is required for access decision ⋆/
1. if $ap \in PIP^{\updownarrow}$ then
2. return False;
3. else if $ap \in AIP^{\downarrow}$ then
4. return True;
5. end if

Comp_Check$_2$ (ap, $\langle CIP, PIP\rangle$)
1. if $ap \in PIP^{\updownarrow}$ then
2. return False;
3. else if $ap \in CIP^{\downarrow}$ then
4. return True;
5. end if

Access Decision (ap, Object O)
/⋆ IPT means intended purpose table ⋆/
1. For each tuple of IPT where Sl_No.= $i(i = 1$ to $n)$
2. c_id=$\prod_{Cus\_ID}$ ($\sigma_{Sl\_No.=i}$(IPT))
3. attr=$\prod_{Attr\_Name}$ ($\sigma_{Sl\_No.=i}$(IPT))
4. if O=$\prod_{Table\_Name}(\sigma_{Sl\_No.=i}$ (IPT)),
attr ∈ {A|A is one of O's attributes}
and c_id∈ $\prod_{O.Cus\_ID}$ (O)
5. ip=$\prod_{Intended\_Purpose}(\sigma_{Sl\_No.=i}$(IPT))
6. if (Comp_Check$_1$ (ap, $\langle AIP, PIP\rangle$)= False)
7. O← $\prod_{attr_1,attr_2,\ldots,attr_n=null}$
($\sigma_{O.Cus\_ID=c\_id}(O)$)
8. else if Comp_Check$_2$ (ap, $\langle CIP, PIP\rangle$)= False
9. O← $\prod_{attr_1,attr_2,\ldots,attr_n=null}$
($\sigma_{O.Cus\_ID=c\_id}(O)$)
10. return O

from access control engine. The access control engine needs a match process to finish the compliance computation fully or conditionally between access purposes and intended purposes. If the requester's access purpose is fully compliant with the intended purposes of requested data, the engine will release full data to the requester. On the other hand, if the access purpose is conditionally compliant, the engine will release conditional data to the requester, otherwise returned data will be null. Thus in this model the search engine needs to evaluate two compliance checks, the first one is for fully compliance and the second one is for conditionally compliance. The compliance computation and the access decision algorithm of the model is illustrated in Table 4. Method Comp_Check returns the result of the purpose compliance check (fully or conditionally) for the given intended purpose with three levels as described in Section 4. Method Access Decision is

based on the Comp_Check and the Intended_Purpose of a particular attribute in the IPT table.

6 Conclusion

Purposes play a significant role in the field of database management system privacy preserving techniques. In this paper we presented a CPBAC and injected it with RBAC which we referred to RCPBAC model that enables enterprise to operate as a reliable keeper of their customers data. The basic concepts of the proposed model is discussed and it has shown the possibility to extract more information from customers by providing a secure privacy policy. We also analyzed an algorithm to achieve the compliance check between access purpose and intended purposes. The effect of the proposed access control can be useful for internal access control within an organization as well as information sharing between organizations as many systems are already using RBAC mechanisms for the management of access permission. This technique can be used by enterprises to enforce the privacy promises they make and to enable their customers to maintain control over their data.

References

1. Agrawal, R., Kiernan, J., Srikant, R. and Xu, Y.: Hippocratic databases. In: 28th International Conference on Very Large Databases, pp. 143-154. Hong Kong (2002).
2. Agrawal, R., Bird, P., Grandison, T., Kiernan, J. Logan, S. and Xu, Y.: Extending relational database systems to automatically enforce privacy policies. In: 21st International Conference on Data Engineering, pp. 1013-1022. Tokyo (2005).
3. Al-Fedaghi, S.S.: Beyond Purpose-based privacy access control. In: 18th Australian Database Conference, pp. 23-32. Ballarat (2007).
4. Barker, S. and Stuckey, P.N.: Flexible access control policy specification with constraint logic programming. ACM Transaction on Information and System Security. 6(4), 501-546 (2003)
5. Bertino, E., Jajodia, S. and Samarati, P.: Data-base security: Research and practice. Information systems. 20(7), 537-556 (1995).
6. Byun, J.W., Bertino, E. and Li, N.: Purpose based access control of complex data for privacy protection. In: 10th ACM Symposium on Access Control Model And Technologies, pp. 102-110. Stockholm (2005).
7. Byun, J.W., Bertino, E. and Li, N.: Purpose based access control for privacy protection in relational database systems. VLDB J. 17(4), 603-619 (2008)
8. Denning, D., Lunt, T., Schell, R., Shockley, W. and Heckman, M.: The seaview security model. In: 1988 IEEE Symposium on Research in Security and Privacy, pp. 218-233, Oakland (1988).
9. Forrester Research: Privacy concerns cost e-commerce $15 billion. Technical report, 2001.
10. IBM. The Enterprise Privacy Authorization Language (EPAL), `http//www.zurich.ibm.com/security/enterprise-privacy/epal`
11. Kabir, M.E and Wang, H.: Conditional Purpose Based Access Control Model for Privacy Protection. In: 20th Australisian Database Conference, pp. 137-144. Wellington (2009).

12. LeFevre, K., Agrawal, R., Ercegovac, V., Ramakrishnan, R., Xu, Y. and DeWitt, D.: Disclosure in Hippocratic databases. In: 30th International Conference on Very Large Databases,pp. 108-119. Toronto (2004).
13. Marchiori, M.: The platform for privacy preferences 1.0 (P3P1.0) specification. Technical report, W3C, 2002.
14. Massacci, F., Mylopoulos, J. and Zannone, N.: Minimal Disclosure in Hierarchical Hippocratic Databases with Delegation. In: 10th Europran Symposium on Research in Computer Security, pp. 438-454. Milan (2005).
15. Rizvi, S., Mendelzon, A.O., Sudarshan, S. and Roy, P.: Extending query rewriting techniques for fine-grained access control. In: ACM SIGMOD Conference 2004, pp.551-562. Paries (2004).
16. Powers, C.S., Ashley, P. and Schunter, M.: Privacy promises, access control, and privacy management. In: 3rd International Symposium on Electronic Commerce, pp. 13-21. North Carolina (2002).
17. Sandhu, R. and Jajodia, S.: Toward a multilevel secure relational data model. In: 1991 ACM Transactional Conference on Management of Data, pp. 50-59. Colorado (1991).
18. Sandhu, R.S., Coyne, E.J., Feinstein, H.L. and Youman, C.E.: Role-based access control models. IEEE Computer, 29(2), 38-47 (1996)
19. Sandhu, R. and Chen, F.: The multilevel relational data model. ACM Transaction on Information and System Security. 1(1), 93-132 (1998)
20. World Wide Web Consortium (W3C).: Platform for Privacy Preferences (P3P), `http://www.w3.org/P3P`
21. Yang, N., Barringer, H. and Zhang, N.: A Purpose-Based Access Control Model. In: 3rd International Symposium on Information Assurance and Security, pp. 143-148, Manchester (2007).
22. Peng, H., Gu, J. and Ye, X. Dynamic Purpose-Based Access Control.In: IEEE International Symposium on Parallel and Distributed Processing with Applications, pp. 695-700, Sydney (2008).
23. Hung, P.C.K.: Towards a Privacy Access Control Model for e-Healthcare Services. In: Third Annual Conference on Privacy, Security and Trust, New Brunswick (2005).