Chapter 3 Proposed Model for policy privacy preservation

3.1 Introduction

In the previous chapter a detailed literature survey about the related database access control models was surveyed in depth, explaining reasons for selecting these models to develop the proposed model. The novel model is an improved model that meets the particular requirements of workflow and non-workflow system in enterprise environment. It is based on the characteristics of the conditional purposes, conditional roles, tasks, and policies. The proposed features of the model features are presented in section 3.2. The proposed model definitions are detailed in section 3.3. In section 3.4 the proposed database model is discussed. The chapter is concluded in section 3.5.

3.2 Features of the proposed model

3.2.1 General in the proposed model

The proposed model allows more information from data providers to be extracted while at the same time assuring privacy that maximizes the usability of consumers' data. It allows users to use some data for certain purposes conditionally.

Consider the following hypothetical database illustrated in Table 3-1.

Table 3-1 Hypothetical database

Name	*Age*	*NameIP*	*AgeIP*
Alice	*24*	*<{M},{A}>*	*<{A},{M}>*
Nora	*45*	*<{M},{A}>*	*<{A},{M}>*

A= {Admin purpose}, M= {Marketing purpose}, IP = {Intended purpose} = < {Allowed intended purpose}, {Prohibited intended purpose}>

Suppose that

- Alice and Nora names could be used for “Marketing” purpose.
- Alice and Nora ages could be used for “Admin” purpose but strictly prohibited to use for “Marketing” purpose.

Consider the following queries

1. “SELECT name FROM Table 3-1 FOR Marketing Purpose”
2. “SELECT name, age FROM Table 3-1 FOR Marketing Purpose”

Applying the previous queries using PBAC model reveals the below [17].

The first query returns the names of Alice and Nora.

The second query returns nothing because prohibited intended purposes override the allowed intended purposes.

PBAC model protects privacy of consumers but in the same time leads to more information loss.

So what if the data can be extracted conditionally without violating customers’ privacy?

In the proposed model another type of the intended purposes IP is adopted, which is a conditional intended purpose that allow us to return data without violating the consumer privacy as follows;

Applying the second query "SELECT name, age FROM Table 3-2 FOR Marketing Purpose”, on the hypothetical database in Table 3-2, and according to Table 3-3, which illustrates some imaginary records and intended purpose stored in a conceptual data base relation. Each data elements stored in three different forms each of which corresponds to a particular intended purpose. So the query will return “A, N” for the name filed and for the age field it will return the data in the conditional form as “20-30, 40-50”.

Table 3-2 Hypothetical database2

Name	*Age*	*NameIP*	*AgeIP*
Alice	*24*	*<{M},{M},{A}>*	*<{A},{M},{M}>*
Nora	*45*	*<{M},{M},{A}>*	*<{A},{M},{M}>*

A= {Admin purpose}, M= {Marketing purpose}, IP = {Intended purpose} = < {Allowed intended purpose}, {Conditional Intended purpose}, {Prohibited intended purpose}>

Table 3-3 Fictional records and intended purposes

	Name	Age
AIP CIP PIP	Ali A *	24 20-30 *
AIP CIP PIP	Nora N *	45 40-50 *
AIP CIP PIP	Lily L *	56 50-60 *

IP = {Intended purpose} = < {Allowed intended purpose}, {Conditional Intended purpose}, {Prohibited intended purpose}>

From the results above, the proposed model allows the "Age" data field to be conditionally used, which gives more information without violating users' privacy.

Another important feature in the proposed model besides extracting the data conditionally is that it applies the Separation of duty policy, consider we need to implement the following tasks in a company; Task1 (Request promotion) and Task2 (Approve promotion). These two tasks could not be assigned to the same role and user because they are conflicting entities. So there is a need for a policy to apply this constrain, which is the Separation of Duty policy. Separation of duty policy is supported by means that two or more different people are responsible for the completion of a task or set of related tasks. The purpose of this principle is to discourage fraud by spreading the responsibility and authority for an action or task over multiple people, thereby raising the risk involved in committing a fraudulent act by requiring the involvement of more than one individual.

The proposed model also applies scope inheritance concept; in traditional TRBAC model [21], the higher role inherits total permissions from lower role. But in the actual application, high role can only inherit some permission or just inherit no permissions. As an implementation in the school hierarchy as shown in Figure 3-1. The school hierarchy is divided into multiple domains, each domain contains several roles, and each role only inherit the permissions form the domains it assigned to. For example Employee1 role in College2 domain can inherit permissions from descendant roles in StaffRoom1 domain and Course1 domain, otherwise Employee2 role in College2 role inherits nothing.

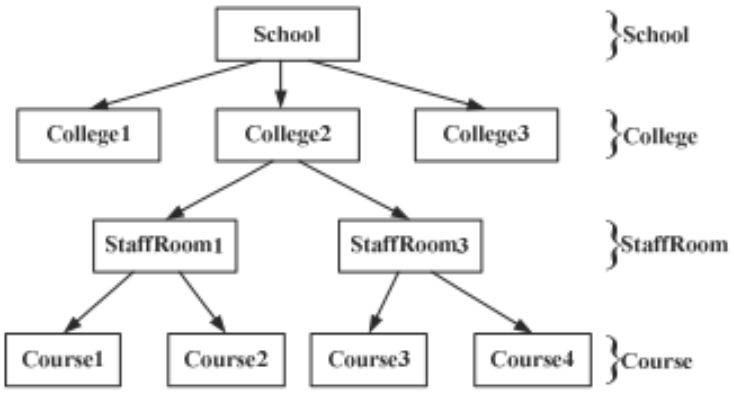

Figure 3-1 School hierarchy scope inheritance

The next subsection introduces the desirable features of the proposed model.

3.2.2 Desirable Features of the Novel Model

The proposed model has the following features listed below.

- Using data conditionally.

  The proposed model allows using data conditionally to release certain information for certain purpose by removing 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 data conditionally, data providers feel more comfortable to release their data. It allows more information from data providers to be extracted while at the same time assuring privacy that maximizes the usability of consumers' data. It allows users to use some data for certain purposes conditionally.

- Workflow and non-workflow systems.

  The proposed model supports workflow and non-workflow systems. It approaches security modeling and enforcement at the application and enterprise level instead of having system centric view of security. It has an active security model, which means that it has active runtime management of tasks progression to completion and permissions assigned to tasks. Permissions are automated by means that activated and deactivated in accordance with emerging context associated with progressing tasks. So the proposed model provides automation for the authorization and self-administering to a great extent, thereby reducing the overhead typically associated with fine-grained subject-object security administration [28] [29].

- Automated permission assignment and revoking.

The proposed model enables the granting, usage tracking, and revoking of permissions to be automated and coordinated with the progression of the various tasks. Without active authorization management, permissions will in most cases be "turned on" too early or too late and will probably remain "on" long after the workflow tasks have terminated. This opens up vulnerabilities in systems. [18].

- Domain inheritance not role hierarchy inheritance.

The proposed model removes role of inheritance in the traditional model by using domains, classifies the roles and tasks according to the actual needs, ensures the system security, and reduces the complexity of the access policy.

- Static and Dynamic authorization.

The proposed model uses policies in static authorization and dynamic authorization; also it applies the Separation of Duty principle. Both SSD (Static Separation of Duty) and DSD (Dynamic Separation of Duty) are enforced to prevent information being misused and prevent fraudulent activities.

- Non-centralized management.

Non-centralized management assigns permissions to multiple managers to share permissions and simplify the work task of permission management despite of having one administrator responsible for permission assignment in the parent role. Each manager has a separate management and must be familiar with the system and is qualified to judge who needs information.

3.3 Proposed Model Definitions

Definition 3.1 (Domain).

Domain allows users to have the system boundary access permission and do not inherit all permission according to their assigned roles. Only inherit permissions from roles inside their domains. Domain provides a flexible way to divide thousands of objects. The domain administrator can divide the domain according to function responsibilities, object type, the geographical location of object. The mainly problem domain can solve is decentralized authority management and grading authorized. Both user-role and permission-role management can realize decentralized management by giving administrator distribution scope appropriately [21].

Definition 3.2. (Domain inheritance).

Roles inside each domain have a hierarchy and according to it, roles inherit permissions from roles inside their hierarchy. As an implementation is the school hierarchy as shown in Figure 3-1. The school hierarchy is divided into multiple domains, each domain contains several roles, and each role only inherit the permissions form the domains it assigned to. For example Employee1 role in College2 domain can inherit permissions from descendant roles in StaffRoom1 domain and Course1 domain, otherwise Employee2 role in College2 role inherits nothing.

Definition 3.3. (Separation of Duty).

Separation of Duty is a security principle used to formulate multi-person control policies, requiring that two or more different people be responsible for the completion of a task or set of related tasks. The purpose of this principle is to discourage fraud by spreading the responsibility and authority for an action or task over multiple people, thereby raising the risk involved in committing a fraudulent act by requiring the involvement of more than one individual. Consider we need to implement the following tasks in a company; Task1 (Request promotion) and Task2 (Approve promotion). These two tasks could not be assigned to the same role and user because they are conflicting entities. So there is a need for a policy to apply that, which is Separation of Duty using policies [25].

Definition 3.4. (Static and Dynamic Separation of Duty).

Compliance with static separation requirements can be determined simply by the assignment of individuals to roles and allocation of transactions to roles. The more difficult case is dynamic separation of duty where compliance with requirements can only be determined during system operation. The objective behind dynamic separation of duty is to allow more flexibility in operations.

3.4 Proposed Database Model

The proposed model use the union between entities of database related work models for privacy preservation.

Figure 3-2 shows the proposed data model stratifying policy privacy preservation.

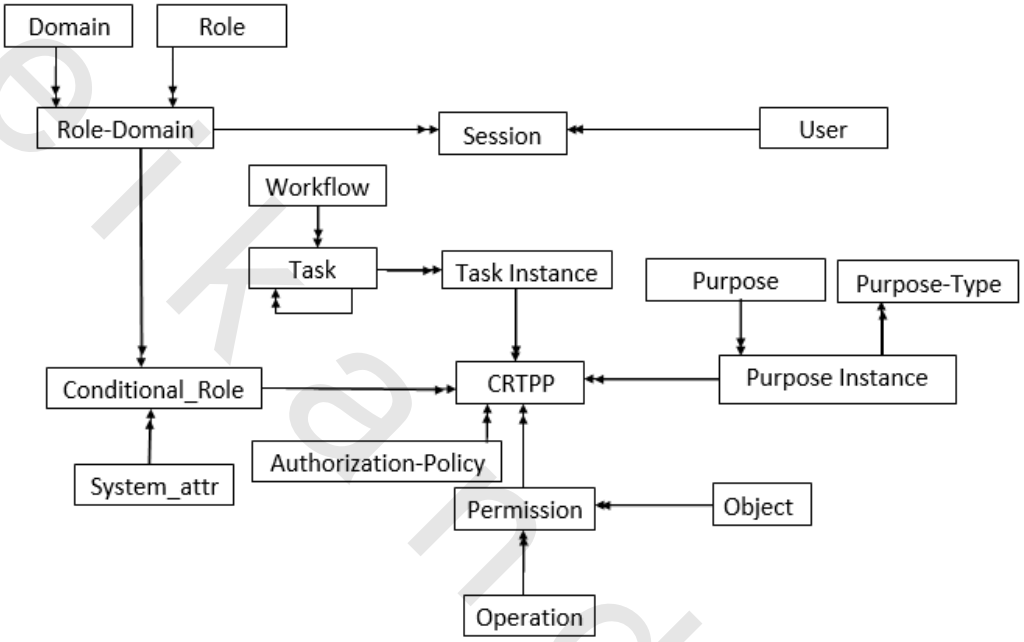

Figure 3-2 The Proposed Database model of policy privacy preservation

In this model, roles are assigned to domains instances, each role-domain instance are assigned to a system condition. Each workflow has some tasks, and each task instances are assigned to conditional roles and purposes. Each roles, tasks and purposes instances are associated with policies. Access rights are associated with conditional roles, tasks and purposes instances.

Model entities.

Role: is a job function or job title within the organization associated with its authority and responsibility.

Domain: roles-scope, system boundary access permission.

User: it can independently access the computer data and resource and it maybe person or application program.

Session: is the mapping between the user and the activated subset of the roles the user assigned to.

Conditional Role: conditions on roles, like system conditions and time conditions.

System_attribute: system condition on roles, roles may be activated only in a specific time interval, or activated for users only logged in from specific machines.

Task: activities in the workflow.

Tasks-Instance: the task instance is a dynamic concept in workflow system and also in an instance of operational task and task execution. Each task includes five status: static status, active status, suspended status, termination status, and failed status [15].

Workflow: group of some business processes.

Purpose: is the reason for accessing the data.

Purpose type: allowed intended purpose, Prohibited intended purpose, and Conditional intended purpose.

Purpose instance: the combination of the purpose and its type.

Policy: a set of policies restricted by the system, for example conflicting entities policy, which means that two conflicting entities should not be assigned to any entity such as receiving checks (payment on account), approving write-offs roles should not be assigned to the same user.

CRTPP: is the relationship between conditional roles, tasks, conditional purposes, and permissions.

Object: database objects like database tables, table columns, and table rows.

Operation: different database operations like query, add, delete, modify, and so on.

Permission: it will grant or deny one or more data in computer system by some way in the range of user access permissions.

From the above data model, it may be deducted that the additional features of the proposed model are satisfied at the cost of imply adding new tuple(s).

3.5 Conclusion

This chapter describes the proposed model features and the need to extend the existing models. The proposed model definitions are introduced and the proposed database model is discussed.

Table 2.4, which represented the existing database access control models is re-visited and the proposed system is added and compared with existing features as shown in table 3.4. The proposed model supports the following features listed in the table below in addition to the features of table 3.4, the proposed model also, enjoys the following standard RBAC features.

- Flexibility.
  The proposed model can be applied simply to any organization or company. The relationship between entities (Figure 3-2) may take care of any changes in the organization privacy preservation policies.

- Simplicity.
  The proposed model is simple to apply with a manageable cost. Simple addition of a new corresponds tuple (s) to the definition of new role(s), task(s), and policy (policies).

- Data quality.
  The proposed model allows the data to be accessed conditionally, which provide more information to be extracted without revealing the real data.

- Safety.
  The proposed model applies security policies like separation of duty policy to provide a high level of security.

Table 3-4 Proposed model versus Existing models surveyed in the related work

Features	CBBAC model	MD-TRBAC model	PBFW model	Proposed model
Task dependency	X	✓	✓	✓
Dynamic permission management	X	✓	✓	✓
Using data conditionally	✓	X	X	✓
Dynamic Separation of duty policy	X	X	✓	✓
Scope inheritance	X	✓	X	✓

√ for supported features. X for un-supported features

The proposed model can be added to the taxonomy presented in figure 2.18. The revised taxonomy is presented in figure 3-3.

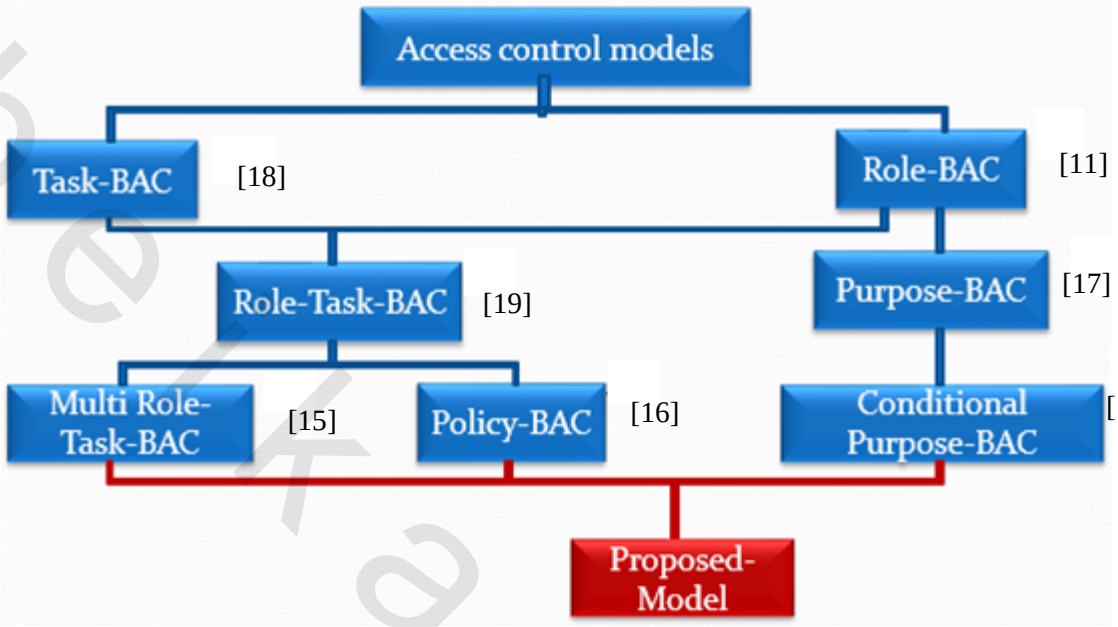

Figure 3-3 Revised taxonomy of the related database access control model and the proposed model

In the next chapter 4, a case study will be performed to evaluate the proposed model.