Chapter 4 Evaluation of the proposed model

4.1. Introduction

In chapter 3, the formal description of the proposed model is discussed in details. The application of the model is illustrated using a case study in section 4.2. In section 4.3 a comparison using the same case study on the related access control models is discussed. Finally, the chapter is concluded in section 4.4.

4.2. Case Study

In this section, the course registration process, illustrated in figure. 4.1, will be implemented using the proposed model. The registration process contains the following four tasks.

- **Task1**: college staff provides course registration forms for students who only met the prerequisites for the course.
- **Task2**: after the end of the course registration period, if the number of the registered students did not meet the minimum number required to open the course then the staff has to make an announcement to drop the course. Otherwise; college staff sends a request to the Professor to confirm the completion of the course registration process,
- **Task3**: professor confirms that the registration process is complete.
- **Task4**: college staff assigns a classroom for the course.

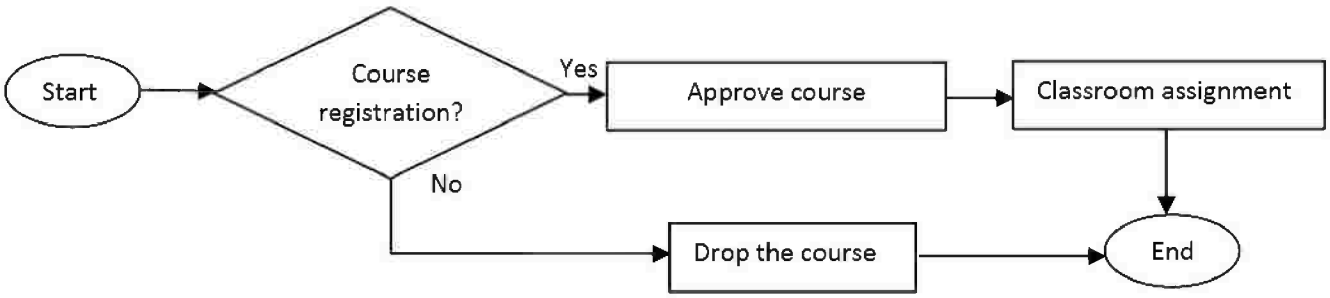

Figure 4-1 Course registration process

The course registration database model is illustrated in Figure 4.2.

Student can register to multiple courses, Professor can teach multiple courses, and many professors can teach the same course, and College staff can assign a classroom for each course.

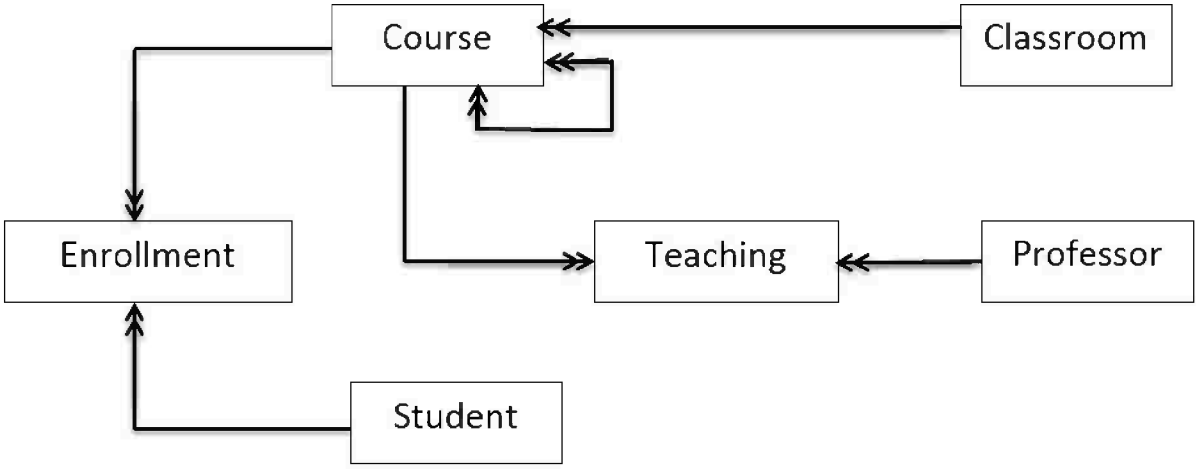

Figure 4-2 Course registration database model

According to the proposed model, roles will be organized in domains. By means that each role will only inherits permissions form the domains it assigned to or it will inherit nothing. Applying the pervious aspect leads us to the college roles hierarchy and domains (group of roles) hierarchy in the following Figure 4.3.

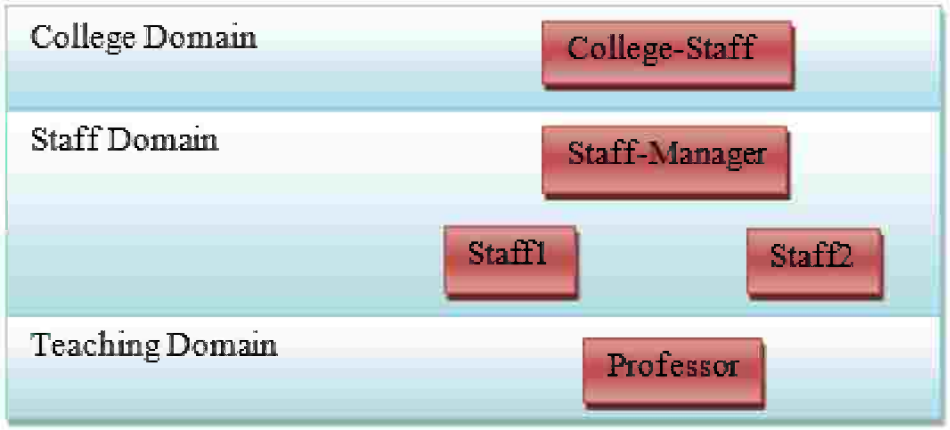

Figure 4-3 College Domain hierarchy

As a result of the domain and roles hierarchy, each role will be assigned to some domains and gain some permissions as in Table 4-1, Table 4-2 and Table 4-3, respectively.

Table 4-1 Roles descriptions

Role title	Role Description
Staff	Responsible for providing course registration forms for students who only met the prerequisites for the course And sending requests to professors to confirm the completion of the registration process, or Send a request to the Staff-Manager to make an announcement to cancel the course if the number of registered students is less than the minimum required to open the course
Staff	Responsible for classroom assignments
Staff-Manager	Responsible for making an announcement to cancel the course because the number of registered student did not meet the minimum number required to open the course
Professor	Manages teaching, writing tests and other teaching assignments.

Table 4-2 Domains and permissions assignment

Domain	Permissions (database access)
Staff Domain	Course, Classroom, and conditional purpose on Enrollment database tables
Teaching Domain	Student, Course, Professor, and Teaching database tables

Table 4-3 Roles and permissions assignment

Role title	Assigned Domain	Permissions (database access)
Staff	Staff Domain, and Teaching Domain	Course, Classroom, Student, Professor, Teaching and Enrollment database tables
Staff	Staff Domain	Course, Classroom database table And conditional access purpose on Enrollment database table
Staff-Manager	Staff Domain	Course, and Classroom database tables. And conditional access purpose on Enrollment database table
Professor	Teaching Domain and Course Domain	Course, Professor, Student, Enrollment and Teaching database tables

According to the registration process requirements and the proposed model.

- **Task4** (Classroom assignment) will not be active until **Task3** (Professor confirms the registration process) is terminated; applying the dynamic permission assignment concept.
- In traditional RBAC model, the higher role inherits total permissions from the lower role. But in the proposed model, roles only inherit the domain permissions it assigned to. Applying role inheritance scope, **Staff-Manager** role is assigned to domain **Staff-Domain** so it will only inherits **Staff-Domain** permissions. In traditional RBAC; **Staff-Manager** will inherit all its descendants' permissions, and according to that **Staff-Manager** will inherit **Teaching-Domain** permissions and **Staff-Domain** permissions, which may lead to information misuse**.**
- In **Task4**(Classroom assignment), **Staff2** has a conditional access purpose on**Task4,** which is to get the count of the registered students to locate a suitable classroom, **Staff2** role does not need a full access on the student database table, all it need is the count of the students.

After the simulation of the implementation of the registration process above on the proposed model, the following aspects and features are discussed.

- The proposed model apply the dynamic permission assignment concept, by means that permissions will be authorized to the user when user needs it not too early or too late.

- Role inheritance scope is applied by the proposed model. Roles will only inherit permissions needed to complete the tasks, and it will not inherit its descendants' permissions as applied in the RBAC model.

- The proposed model makes a full use of the data without violating the privacy by applying the notion of the conditional purposes. Conditional purposes provide extracting more information from the same data while at the same time assuring privacy that maximizes the usability of consumers' data.

- After each task completion, its permissions will be revoked automatically, which provides more security to the system.

- After each task completion, its permissions will be revoked automatically.

4.3. Comparison to the related database access control models

4.3.1. CPBAC course registration process

Simulating the implementation of the course registration process on the CPBAC model, consider the following College roles below.

- **Role Title: staff-A.**

  Responsible for providing course registration forms for students who only met the prerequisites for the course, and sending requests to professors to confirm the completion of the registration process, or Send a request to the Staff-Manager to make an announcement to cancel the course if the number of registered students is less than the minimum required to open the course.

- **Role title: staff-B.**
  Responsible for classroom assignments.

- **Role Title: staff-Manager.**

  Responsible for making an announcement to cancel the course because the number of registered student did not meet the minimum number required to open the course.

- **Role Title: professor.**
  Manages teaching, writing tests and other teaching assignments.

Each Role has the following permissions below.

Table 4-4 CPBAC Role permissions assignment

Role title	Permissions (database access)
Staff-A	Course, Classroom, Student, Professor, Teaching and Enrollment database tables
Staff-B	Course, and Classroom database tables. And conditional access purpose on Enrollment database table
Staff-Manager	Course, Classroom, Student, Professor, Teaching and Enrollment database tables. And conditional access purpose on Enrollment database table
Professor	Course, Professor, Student, Enrollment and Teaching database tables

There is no notion of tasks on CPBAC, so permissions are given directly to roles as the following permissions below.

- **Staff-A** provides course registration forms for students who only met the prerequisites for the course**.**
- After the end of the course registration period, **Staff-A** checks the number of registered students; if it is more than the required number to open the course, send a request to Professor to approve. If the number of registered student less than the minimum number required to open the course, send a request to the **Staff-Manager** to make an announcement to cancel the course the number of registered student less than the minimum number required to open the course.
- **Staff-Manager** to make an announcement to cancel the course.
- **Professor** approves the course registration process if the number of registered students is more than the required number to open the course.
- **Staff-B** assigns a classroom for the course.

4.3.2. Comparison to CPBAC

Comparing the results of implementing the course registration process on the proposed model and the CPBAC model leads to the following results listed below.

- **Domain inheritance not role hierarchy inheritance.**
  The proposed model applies domain inheritance concept CPBAC model applies the role inheritance concept. Domain inheritance concept means that any role will only inherit permissions form the domain it assigned to, not from its descendants roles.
  Example: on the proposed model "**Staff-Manager**" role will only have **"staff-domain**" permissions, so the "**Staff-Manager**" role will gain access to "Course" and "classroom" database tables and conditional access purpose on "Enrollment" database table. On the other side CPBAC model does not have the notion of the domain inheritance and the "**Staff-Manager**" role will inherits all its descendants' roles permissions; So it will gain access to "Professor", "Teaching", "Student", "Enrollment", "Course" and "classroom" database tables. The difference between the "**Staff-Manager**" role implementation in the proposed model and CPBAC model is that it will gain extra access to "Professor", "Teaching", "Student" and "Enrollment "database tables.

- **Automated permission assignment and revoking.**
  The proposed model will give access to the "**Staff**" role to do the "classroom assignment" task, only if the "student registration process" task is done and complete. On the other side the CPBAC model grant permission to the "**Staff**" role even if the registration process task failed for any reason. In the CBRBAC model there is no notion of a task or permission assignment automation; Granting and revoking permissions is done manually by system administrator.

- **Workflow systems.**
  The proposed model supports workflow systems. 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. On the other side the CPBAC model does not support the workflow systems and does not know the notion of a task.

From the comparison above and the results of table 4-5, CPBAC model does not support the workflow systems. CPBAC model has a manual permission assignment, and give extra access to roles by applying the role inheritance concept, which may lead to information misuse.

Table 4-5 Comparison between the proposed model and CPBAC model

Role	CPBAC Permissions	Proposed model Permissions	Comments
Staff1	Course	Course	
	Classroom	Classroom	
	Student	Student	
	Enrollment	Enrollment	
	Professor	Professor	
	Teaching	Teaching	
Staff2	Course	Course	**No notion of lifecycle** in CPBAC **and no automation** to check the course registration period, **permissions are given too early or too late**
	Classroom	Classroom	
	Enrollment	Conditional access on Enrollment	
	Student		
Staff-manager M	Course	Course	CPBAC give Staff-Manager **extra permission** (Student, Enrollment, Professor and Teaching tables), no notion of domain
	Classroom	Classroom	
	Student		
	Enrollment	Conditional access on Enrollment	
	Professor		
	Teaching		
Professor P	Course	Course	**No notion of lifecycle** in CPBAC period**, permissions are given too early or too late** to approve the course requests.
	Professor	Professor	
	Teaching	Teaching	

4.3.3. MD-TRBAC course registration process

Applying the course registration process on MD-TRBAC model, consider the following College roles and domain permission assignment in table 4-6 and table 4-7, respectively.

Table 4-6 Roles descriptions MD-TRBAC model

Role title	Role Description
Staff	Responsible for providing course registration forms for students who only met the prerequisites for the course And sending requests to professors to confirm the completion of the registration process, or Send a request to the Staff-Manager to make an announcement to cancel the course if the number of registered students is less than the minimum required to open the course
Staff	Responsible for classroom assignments
Staff-Manager	Responsible for making an announcement to cancel the course because the number of registered student did not meet the minimum number required to open the course
Professor	Manages teaching, writing tests and other teaching assignments.

Table 4-7 Domain permission assignment MD-TRBAC model

Domain	Permissions (database access)
Staff Domain	Course, Classroom, and conditional purpose on Enrollment database tables
Teaching Domain	Student, Course, Professor, and Teaching database tables

Each role will gain some permissions as in table 4-8;

Table 4-8 Role permission assignment MD-TRBAC model

Role title	Assigned Domain	Permissions (database access)
Staff	Staff Domain, and Teaching Domain	Course, Classroom, Student, Professor, Teaching and Enrollment database tables
Staff	Staff Domain	Course, Classroom database table And conditional access purpose on Enrollment database table
Staff-Manager	Staff Domain	Course, and Classroom database tables. And conditional access purpose on Enrollment database table
Professor	Teaching Domain and Course Domain	Course, Professor, Student, Enrollment and Teaching database tables

The registration process contains four tasks.

- **Task1**: college staff provides course registration forms for students who only met the prerequisites for the course.
- **Task2**: after the end of the course registration period, if the number of the registered students did not meet the minimum number required to open the course then the staff has to make an announcement to drop the course. Otherwise; college staff sends a request to the Professor to confirm the completion of the course registration process,
- **Task3**: professor confirms that the registration process is complete.
- **Task4**: college staff assigns a classroom for the course.

4.3.4. Comparison to MD-TRBAC

- **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. It allows more information from data providers to be extracted while at the same time assuring privacy that maximizes the usability of consumers' data.
  Example: in the proposed model, "**Staff-2**" role has the classroom assignment class, which needs access to the "**Enrollment**" database table just to get the count of the registered student to find the suitable classroom for them. This task does not need a full access in the "**Enrollment**" database table, for this reason the "**Staff-2**" role has a conditional access purpose on the "**Enrollment**" database table when the classroom assignment is active. On the other side the MD-TRBAC model does not have the notion of using the data conditionally so it will have full access to the "**Enrollment**" database table, which violates the student privacy.

From the comparison above and the results of table 4-9, MD-TRBAC model doesn't have the notion of using the data conditionally. MD-TRBAC model gives the user full access on the data, even if the user needs to make some statistical operations and does not need to get the actual data.

Table 4-9 Comparison between the proposed model and MD-TRBAC model

Role	MD-TRBAC Permissions	Proposed model Permissions	Comments
Staff1	Course	Course	
	Classroom	Classroom	
	Student	Student	
	Enrollment	Enrollment	
	Professor	Professor	
	Teaching	Teaching	
Staff2	Course	Course	**No notion of purposes, and conditional purposes** so Staff2 has full access to Enrollment table, which violates student privacy
	Classroom	Classroom	
	Enrollment	Conditional access on Enrollment	
Staff-manager M	Course	Course	**No notion of purposes, and conditional purposes** so Staff2 has full access to Enrollment table, which violates student privacy
	Classroom	Classroom	
	Student	Student	
	Enrollment	Conditional access on Enrollment	
Professor P	Course	Course	
	Professor	Professor	
	Professor-Course	Professor-Course	

4.3.5. PBFW course registration process

Applying the course registration process on PBFW model, consider the following College roles and domain permission assignment in table 4-10;

Table 4-10 Roles descriptions PBFW model

Role title	Role Description
Staff	Responsible for providing course registration forms for students who only met the prerequisites for the course And sending requests to professors to confirm the completion of the registration process, or Send a request to the Staff-Manager to make an announcement to cancel the course if the number of registered students is less than the minimum required to open the course
Staff	Responsible for classroom assignments
Staff-Manager	Responsible for making an announcement to cancel the course because the number of registered student did not meet the minimum number required to open the course
Professor	Manages teaching, writing tests and other teaching assignments.

The registration process contains four tasks.

- **Task1**: college staff provides course registration forms for students who only met the prerequisites for the course.
- **Task2**: after the end of the course registration period, if the number of the registered students did not meet the minimum number required to open the course then the staff has to make an announcement to drop the course. Otherwise; college staff sends a request to the Professor to confirm the completion of the course registration process,
- **Task3**: professor confirms that the registration process is complete.
- **Task4**: college staff assigns a classroom for the course.

4.3.6. Comparison to PBFW

- **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. It allows more information from data providers to be extracted while at the same time assuring privacy that maximizes the usability of consumers' data.
  Example: in the proposed model, "**Staff-2**" role has the classroom assignment class, which needs access to the "**Enrollment**" database table just to get the count of the registered student to find the suitable classroom for them. This task does not need a full access in the "**Enrollment**" database table, for this reason the "**Staff-2**" role has a conditional access purpose on the "**Enrollment**" database table when the classroom assignment is active. On the other side the MD-TRBAC model does not have the notion of using the data conditionally so it will have full access to the "**Enrollment**" database table, which violates the student privacy.

From the comparison above and the results of table 4-13, PBFW model doesn't have the notion of using the data conditionally and does not apply the scope inheritance concept. PBFW model gives the user full access on the data, even if the user needs to make some statistical operations and does not need to get the actual data.

Table 4-11 Comparison between the proposed model and MD-TRBAC model

Role	MD-TRBAC Permissions	Proposed model Permissions	Comments
Staff1	Course	Course	
	Classroom	Classroom	
	Student	Student	
	Enrollment	Enrollment	
	Professor	Professor	
	Teaching	Teaching	
Staff2	Course	Course	**No notion of purposes, and conditional purposes** so Staff2 has full access to Enrollment table, which violates student privacy
	Classroom	Classroom	
	Enrollment	Conditional access on Enrollment	
Staff-manager M	Course	Course	**No notion of purposes, and conditional purposes** so Staff2 has full access to Enrollment table, which violates student privacy
	Classroom	Classroom	
	Student	Student	
	Enrollment	Conditional access on Enrollment	
Professor P	Course	Course	
	Professor	Professor	
	Professor-Course	Professor-Course	

4.4. Conclusion

This chapter simulates the implementation of a course registration process in a college on the proposed model. Then the same registration process is applied to the CPBAC, MD-TRBAC, and PBFW model. Finally a comparison is made between the proposed model and the related models. In the next and final chapter, there will be a brief discussion of the work that has been done along with this thesis, conclusions, and suggested future work.