SECURITY OF HEALTHCARE SYSTEM USING ROLE-BASED ACCESS CONTOL

Khin Myaing Myaing Tun, Thi Thi Soe Nyunt
University of Computer Studies, Yangon
dawgyi@gmail.com

ABSTRACT

Today, security is recognized as an absolute need in application development. The healthcare sector deals with very sensitive data, patient's medical records need to be kept confidential; hence, security is very important. Role Based Access Control (RBAC) is increasingly used for ensuring security and privacy in complex organizations such as healthcare institutions. This papers is implemented the database security system by using RBAC for the patient treatment information. In this system, the employees of the hospital such as Head of Hospital, Doctors, Sisters, Nurses, Lab staffs and others are defined their role and access right for each role in order to access the treatment information. To improve better security within the system, this system can also control to the sensitive data by controlling attributes using RBAC. The main concept underlying this system uses the RBAC to control unauthorized access to patient medical information.

1. INTRODUCTION

Computer security is the protection of the confidentiality, integrity and availability of automated information. Security mechanisms are used to prevent all the security services that are provided in computer system and networking. Today, most of these security mechanisms are used by computer systems for authentication, access control, audit trail and cryptography. [5]

In a traditional medical system, the protection of patient records information is the responsibility of individual institutions such as hospitals, medical centers, physicians and nurses. Now using highly information technologies such as the Internet, World Wide Web and high-speed networking, patient information can be shared among patients, physician's offices and other related organizations.

This will bring health care industry to move towards to a more open medical information infrastructure and to improve the quality of health care. At the same time, health care industry also presents a number of new challenges in enforcing patient medical information to keep it in confidentiality and availability. This healthcare system requires integrated security management techniques to prevent the existence of serious potential breaches of privacy and security.

RBAC is a security model that restricts system access to authorized users and has been in existence in one form or another since1992 (Ferraiolo and Kuhn, 1992). This model focuses on roles, permissions, users and constrains. Roles are defined for various job functions. Permission is an approval or one or more operations on objects in the system. Users can be assigned one or many roles, and a role can be assigned to one or many users. A role can also have one or much permission assigned to it, and permission can be assigned to one or many roles. [3]

2. BACKGROUND THEORY

The concept RBAC has been used with a multi-user computer system and multi-application online system since the late 1960s and early 1970s. However, RBAC has rapidly emerged in the 1990s as a promising technology for managing and enforcing security in large-scale enterprise-wide systems, largely because of the non-existing enhancement in the traditional Mandatory Access Control (MAC) and Discretionary Access Control (DAC) used in many computer systems and networks. Thus, RBAC is an alternative to traditional MAC and DAC policies that is currently attracting increasing attention, particularly for commercial applications. [7]

RBAC is a family of reference models in which permissions are associated with roles, and users are assigned to appropriate roles. This greatly simplifies management of permissions. Roles are created for the various job functions in an organization and users are assigned roles based on their responsibilities 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. Besides that, permissions can be revoked from roles if necessary.[1]

A major purpose of RBAC is to facilitate access control administration and review. This RBAC idea greatly simplifies management of authorization while providing opportunities with great flexibility in specifying and enforcing enterprise-specific security policies, and for streamlining the security management process. [9]

3. SYSTEM OVERVIEW

This healthcare system is divided into two major section, i.e. Administer section and Users section.

Administer section involves control over components such as roles, users and permissions. These include creations, updating and deletion of roles, creations and deletion of users, assignment of user to role and their removal, creation, updating and deletion of permission, assignment of permission to roles and their removal. Administer can define the assignment of user to ward for better security of the patient treatment record. All doctors and nurses in this hospital do not premise to access all of the patient data. They only premise to access with their corresponding patient data. For example, a baby is admitted for treatment in child ward. This patient data is not allowed to access from other medical staff they are assigned to duty in other wards. This treatment data only premise to access doctors and nurses they are assigned to duty in child ward.

This system also shows how attributes can be applied to RBAC, in order to filter the attribute list. To improve better security to the treatment data, doctors and nurses allowable attribute for same filename nay not be the same. For example, a doctor role can be created within a database that allows a user with that role to have read, write access to all columns in a treatment table. However, nurse role can be allowed to have only read access to some column in the same table.

This system maintains a treatment history for each patient. This treatment history typically contains a record of all treatment, lab result, ultrasound result, X-ray result, diagnosis, sign and symptom, drug usage, surgery case and etc.

In the user section, each user enters into the system using his/her username and password. If the user is not valid user, the system shows the error message. If the user is the valid one, the system allows this user to access the patient treatment record with his/her corresponding role and access right. If the user is allowed to have read access of all user accessible files within the database, he can only read all of the patient data.

4. IMPLEMENTATION OF THE SYSTEM

This system intends to implement data security by using role based access control.

4.1. Role defined in the System

According to the role base access control system, this system is based on 12 roles for the whole hospital staff. Moreover, the system will perform for 13 types of the hospital's files. Figure 1 illustrate for accessible files list. Roles are defined according to the job functions. All users in this system can perform their duties through these 12 roles completely by easily log on their correct user name and password. The implementation of RBAC-roles is shown in the following table 1.

Accessible File List

1. Patient Registration File
2. Medical Check-Up File
3. Treatment File
4. Disease File
5. Drug File
6. Dose File
7. Drug Usage File
8. Procedure File
9. Lab File
10. Ultrasound File
11. X-Ray File
12. UserInWard File
13. Ward File

Figure.1. Accessible Files

Table 1. Implementation of RBAC- roles

Role ID	**User Position**
R1+R6	Head of Hospital
R2	Receptionist
R3	Administrator
R4+R6	Ward By Doctor
R5	First Assistant Doctor
R6	Assistant Doctor
R7+R8	Sister
R8	Nurses
R9	Anaesthetize
R10	Lab
R11	X-Ray
R12	Ultrasound

This system allows multiple roles assignment. Users can be assigned more than one role in this system. In the system, Role 1 is granted to User 1(Head of Hospital). However, according to the requirement of the work nature User 1(Head of Hospital) can be assigned another Role 6. So User1 possess to R1 and R6.

4.2. Representation of RBAC with Access Right and Resources

A user is assigned to a role that enables him or her to perform only what is required for that role. In this system, each role contains their accessible files, attribute list and the set of access rights needed for that role. According to the requirement of organizational policy, the attributes of the file may not be the same for all roles. Example of Role ID, their accessible file and attribute lists and corresponding access right are shown in the following table 2.

Table.2. Example of role id and their accessible file, attribute list and access right

RoleID	Accessible File	Attribute List	Access Right
R1	Patient	PatientID	R
		Patient Name	R
		Age	R
		FatherName	R
		BloodGroup	R
		DrugAllergy	R
		WardID	R
		RegDate	R
	Medical check	MedicalcheckID	R
		MedicalcheckDate	R,I,E
		Height	R,I,E
		Weight	R,I,E
		PastHistoy	R,I,E
		Smoking	R,I,E
		Eyes	R,I,E
	Treatment	TreatmentID	R
		TreatmentDate	R,I
		PatientID	R,I
		DiseaseID	R,I
		WardID	R,I
		SignSymptom	R,I
		Diagnosis	R,I
		SurgeryCase	R,I
		Remark	R,I
	Lab	LabID	R
		LabDate	R
		LabResult	R

R=Read, I=Insert, E=Edit, D=Delete

4.3. Process Flow of the System

The system has two types of user such as normal user and administrator. Either normal or administrator user enter into the system by input user name and password. Then the system checks for authorization.

If the user is the valid normal user, the system then collects its role and corresponding granularity information and produces accessible menu list. The user can perform the desired duty completely by selecting relevant menu. When the user selects the relevant menu, the system checks the permission of attribute list for each file name for each role. If the check permission is valid, the system displays the corresponding data. Then the user can perform updating operation on the file. If the check permission is invalid, the system display the error message and the user log out from the system.

If the admin user log into the system, he/she is checked for authorization. The authorization process is similar to the authorization for user level user. If the user is valid admin user, he is shown the corresponding admin level menu. Then he can make create role, update role, delete role, create user, and delete user and user to role assignment. The process flow of the system is shown in the follow figure 2.

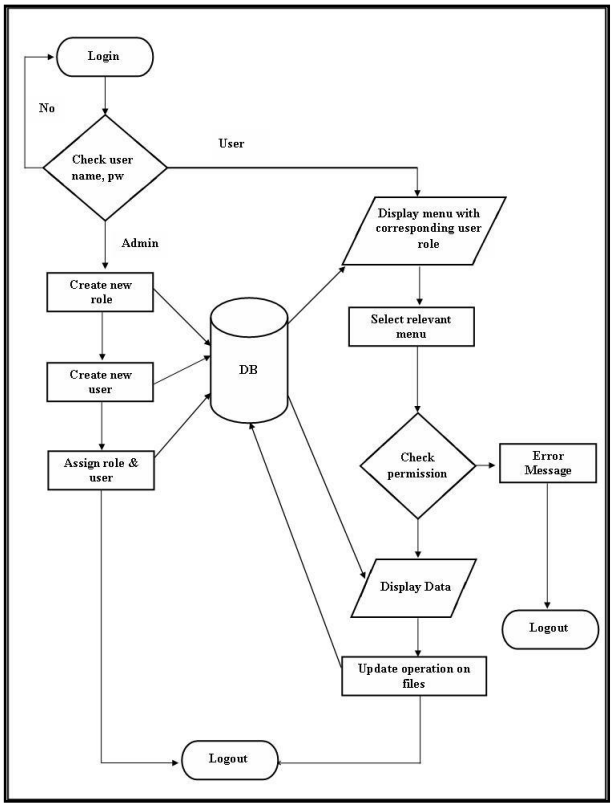

Figure.2. The Process Flow of The System

5. EXPERIMENTAL RESULT

The implementation of this system mainly performs two types of section, i.e. Administer section and Users section.

5.1. Administer Section

Firstly, the administer is checked for authentication. The check authentication function operates as follows: a user presents his/her user name and password. If the user is not valid, the system returns error message. If the user is the valid one, the system displays correct message. Either administrator or data user can perform their associated tasks after a successful authentication.

Administrator can create the new role by defining the role definition. The system checks it for existing one. If not existing one, saves the role definition with the defined role name and otherwise shows the error message to the user. User Interface design for create new role and role definition frame is shown in following figure 3.

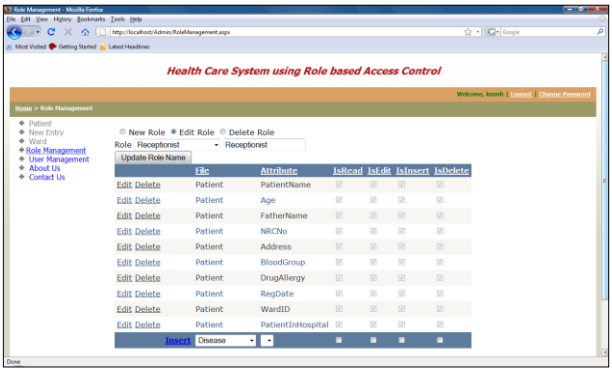

Figure.3. Interface for role definition frame

The administrator can also assign the new user to role. This system allows multiple roles assignment. Users can be assigned more than one role in this system. The assigned user must get the access granularity according to their assigned role. After the user and role assignment, the administrator can assign to this user with their corresponding ward according to better security. However, administrator does not permit to assign the user roles, attribute lists and access rights. Roles with their granularity are defined according to the job function and work nature. Interface design of the user, multiple role and ward assignment is shown in the following figure 4.

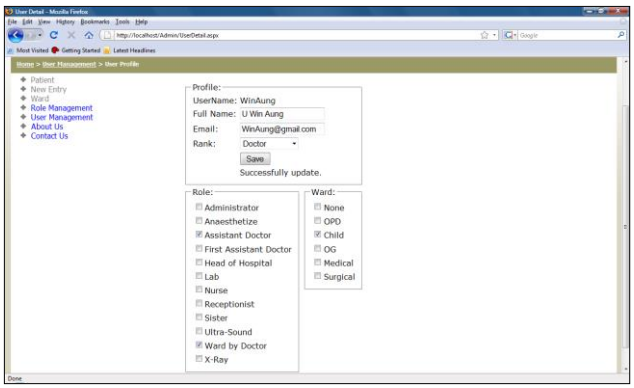

Figure.4. Interface design for multiple role assignment

5.2. User Section

Firstly, the user is checked for authentication. The authorization process is similar to the authorization for the administer.

5.2.1. Viewing the patient treatment history

The assistant doctor permits to access detail patient treatment data. Figure 5 illustrates the interface of viewing the treatment history for assistant doctor.

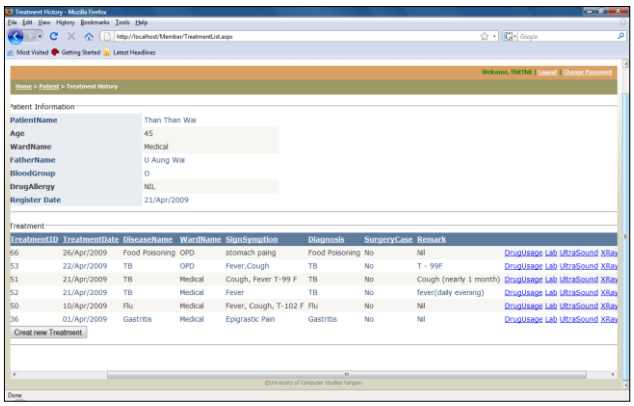

Figure.5. Viewing a patient treatment history for assistant doctor

In hospital, nurses are assigned their task by the doctor. They do not permit to know detail patient treatment record. In this system, they can only read and write at the drugusage data. Although nurses can not view all of the treatment history, the assistant doctors can view the detail patient treatment history (in figure 5). Interface design for viewing the patient treatment for nurse is shown in the following figure 6.

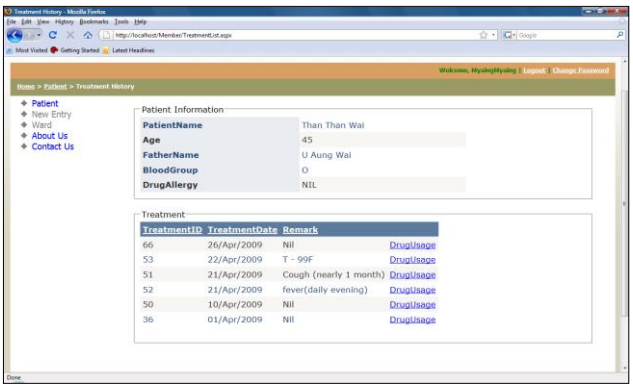

Figure.6.Viewing a patient treatment history for nurse

5.2.2 Inserting the new treatment record

If the user request is inserting data to file, the system shows the blank form for inserting new data. Then the user fills the new information. Figure 7 illustrates for inserting the new treatment record.

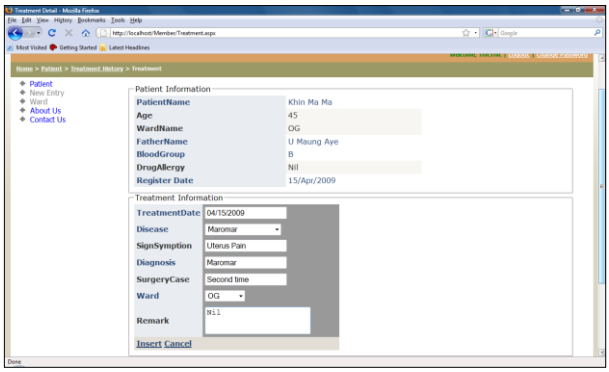

Figure.7. To insert the new treatment

5.2.3. Updating the patient personal data

If the patient personal data change, the receptionist can allow updating this data at registration form. If the receptionist presses the edit button, the system shows the frame of updating form with old information. Then the receptionist can update the desired field. The interface design for updating file is shown in the following figure 8.

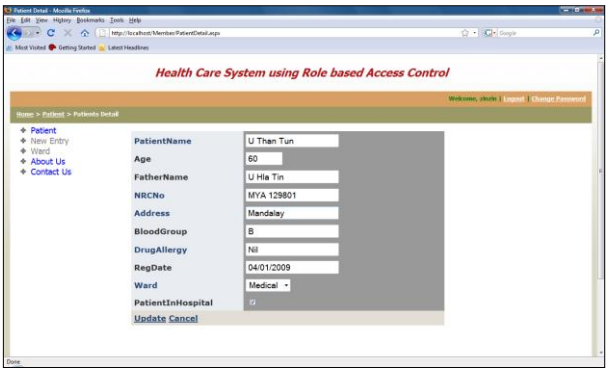

Figure.8. To update the patient personal data

5.2.4. Deleting a patient from the patient list

If the receptionist request is deleting data that is requirement of the work nature, the system shows the confirmation message to user. Then the receptionist presses on the 'yes' button, the data is deleted. Figure 9 displays interfaces for deleting data.

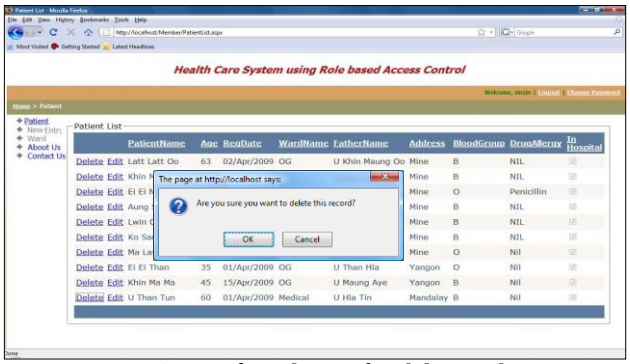

Figure.9. Interface design for deleting data

6. CONCLUSION

With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. This system allows the multiple role assignment for the users. In this system, roles are defined for various job function and users are assigned roles based on their responsibilities and qualifications. Role definition can be established when new operations are instituted, and old operations can be deleted as organizational functions change and evolve.

To improve better security within the system, this system can also control to the sensitive data by controlling attributes using RBAC.

As a result, Organization may increase their confidence in their computer systems and be able to increase the sharing of resources, being less concerned about potential security violations**.**

REFERENCES

[1] David F., David R., Janet A., "Role-Based Access Control models*": IEEE Computer*, Feb 1996

[2] David F., "An Introduction to Role-Based access Control": NIST/ITL Bulletin, December 1995

[3] D. Ferraiolo, D. and Kuhn, R. 1992, 'Role-Based Access Control', 15th National Computer Security Conference

[4] R.Sandhu et al., "Role-Based Access Control". *IEEE Computer*, Vol.29,No 2, February 1996

[5] R.Sandhu et al., "The RRA97 Model for Role-Based Administration of Role Hierarchies", *in Proceeding of 14th Annual Computer Security Application Conference*, 1998

[6] R.Sandhu et al., "The ARBAC97 Model for Role-Based Administration of Roles", *ACM Transaction on Information and System Security*, Vol12, No.1, February 1999

[7] R. Sandhu et al., "Role-Based Administration of User-Role Assignment: The URA97 Model and Its Oracle Implementation". *The journal of Computer Security*, 1999

[8] R. Sandhu et al., "The ARBAC97 Model for Role-Based Administration of Roles: Preliminary Description and Outline". *In Proceeding of 2nd ACM Workshop on Role-Based Access Control, Fairfax,* VA, 6-7 November 1997.

[9] R. Sandhu et al., "The URBAC97 Model for Role-Based User –Roles Assignment": Preliminary Description and Outline". *In Proceeding of IFIP WG*