Role Based Access Control in Learning Management System(LMS)

Su Su Yin
Department of Computer Science
University of Computer Studies Taungoo
Taungoo, Myanmar
susuyin@ucsy.edu.mm

Khine Moe Nwe
Faculty of Computer Science
University of Computer Studies Yangon
Yangon, Myanmar
khinemoenwe@ucsy.edu.mm

***Abstract*— During the Corona virus pandemic, we should change for learning classroom system to distance learning (online learning) system. Online learning management system is so flexibility for teaching and learning environment. Learning management system is widely used in the whole world because of saving money, reducing time and more convenience for students. Nevertheless, it is important to protect the information and all other resources from unauthorized access. Role based access control (RBAC) is a powerful mechanism and most suitable approach to provide information security any system. In this paper, the combinations of Core RBAC and Dynamic Separation of Duty RBAC model is proposed and implemented the role based access control learning management system. Moreover, different roles are considered for protecting un-authorization process of the learning management system. Therefore, this paper will be supported to effectively control the accessible data and can strength information security of the system.**

Keywords: LMS, Access Control, RBAC, Core RBAC, Dynamic Separation on duty, Security

I. INTRODUCTION

In the digital campus, learning management system is also very important as a subsystem. By using role based access control method, the learning management system can solve the security issues such as unauthorized person access the secure data. Through the analysis of system permissions and users role, the secure data can be acquired. The basic idea of role based access control is that role are created and then the particular user is assigned appropriate role to get his permissions. Therefore, the user has a role (or several roles) which gives him predefined permissions.

The combination of Core RBAC and dynamic separation of duty (DSD) RBAC model is proposed. By applying the proposed role based access control model, we can achieve the strengthening access control and solve the security issue in learning management system. A learning management system (LMS) is an application for teaching and learning programme such as serving notification, share data, assessment, delivery of courses. LMS is the powerful engine for online learning and it consists of two separate parts: (1) Component of the server that performs the main capability (user authentication, role creating, manage users, delivering courses, serving data and reporting, etc.) (2) User interface that operates using browser as the web by administrators, teachers and students.

When the users log in the system, they must be firstly authenticated identity through the authentication process to get their roles and then role based access control model checks users' rights assigned on their role. In this paper, multiple users can have the same role, and a single user can have a variety of roles. Two requirements for creating the users' role in the learning management system are following: (1) According to the organizational structure, the roles are created by administrator. (2) Each role has their own a unique identify number and user's information of the role saved into the database. Basically, a role based access control model consisted of user, role, session, permission, operation and object. Role is a job function with associated actions and responsibilities conferred to the user within an organization. User is a person who needs to be authenticated and interacts with the system. Permission is officially allowing to perform an operation on secure objects. Object is the any resource of system which can be controlled to access by user (For Example: file, program and database record, etc.) Operation means some functions for the user to execute file or program on a computer. A session is a particular occasion of a user to activate role in which the user is assigned. A user can have multiple sections with different window at the same time.

This paper is composed in the following way. In section 2, we discuss related work. In sections 3, we introduce the RBAC Model and Levels. In section 4, we describe the proposed RBAC Learning Management System using with figures. Finally, we conclude this paper in section 5.

II. A Review of Related Work

Separation of duties, least privilege and data abstraction are three well-known security principles supported by role based access control. Least privilege means only the minimum access should be granted to perform an operation for the minimum amount of time. Least privilege in role based access control can be configured that members of role conduct permissions for the necessary tasks are assigned to the role. Separation of duties means the separation by sharing of more than one individual in one single task. To complete a sensitive task, mutually exclusive roles must be invoked such as a staff of department and a head of department to participate in a task. Data abstraction defines abstract permissions such as operation system provides read, write and execute permissions [5,6].

Role based access control (RBAC) could achieve the requirements of system security and performed better control access and protected system in operation security. RBAC policy means a user is allowed to perform the function based on access control decisions within an organization. The responsibilities of security administrator are to enforce policy and to represent the organization. A lot of researchers have published the implementations of RBAC model. RBAC provides the web based application security. RBAC is a powerful mechanism to reduce the complexity of user assignment and mistake permissions within the organization [11]. Chia-Chu Chiang and Coskun Bayrak [7] studied RBAC's behavior and detail discussed about the policy of RBAC. More specifically in [7], Chia-Chu Chiang and Coskun Bayrak analyzed user role analysis, object privilege

analysis, design of role privilege management scheme and assign system privilege. Joon S. Park[13] gave a way to implement RBAC on the Web by using an Lightweight Directory Access Protocol in the server-pull architecture . Dharmendra Choukse and Umesh Kumar Singh[2] studied the RBAC with Single Sign-on Architecture(SSO) using web service for LMS. Single Sign-on Architecture is an access control mechanism. To reducing extra logins when the user switches applications within one session, SSO supports authentication of a user's access control several software system.

III. RBAC Model and Levels

The stable set of RBAC feature has standardization which can be provided a multiplicity of benefits. Role-based access control (RBAC) is the user assigned permissions through the role by directly to the authorization role to control user's access to the system operation. The definition of the role is a collection of permissions that user can operate in the system. The different roles can be based on the different user's positions or functions when grant the roles. The system can also comparatively uncomplicated to change the user's role. As RBAC model are organized three levels, the functional specification of each level described in Table (1).

Table I. RBAC Model Levels and Functional Specifications

Level	**RBAC Model**	
	Model Level Name	***RBAC Functional Specifications***
1	$RBAC_0$ (Core RBAC)	-Users' permissions acquire through roles -Must supports many to many users assigns roles -Must supports many to many roles assigns permissions -Permissions of multiple roles can be used by users at the same time.
2	$RBAC_1$ (Hierarchical RBAC)	$RBAC_0$ + Role Hierarchical - Must supports role hierarchy (1) General role hierarchies: to serve as role hierarchy, to include user membership among roles and multiplicity permissions' inheritances (2) Limited role hierarchies: defined restrictions in a simpler tree structure (hierarchy of user membership is limited as trees, hierarchy of the role permissions are as inverted trees)
3	$RBAC_2$ (Constrained RBAC)	$RBAC_0$ + $RBAC_1$ + Separation of Duties -Must enforces separation of duties (SOD) -A single duty is distributed among several users. -Well-known two security practices are: (1) Static Separation of Duty (2) Dynamic Separation of Duty

RBAC standard will support researchers with a well-defined fundamental mechanism for creative access control and authorization management models and techniques[11]. Four basic components contain in this model. There are a set of users, a set of roles, a set of permissions and a set of sessions. The user assignment (UA) function is users assign to roles and the permission assignment (PA) function is permissions assign to roles.

A. Core RBAC

Core RBAC contains the main aspects of RBAC, so that it is required in any RBAC system. Core RBAC captures basic concept of RBAC such as assigns users to roles, assigns permissions to roles, and users obtain permissions only if members of roles. Core RBAC includes necessary conditions that many to many assign user-role and permission-role. Therefore, each user can be assigned to one or many roles and each role can have more than one user. Similarly, each permission can be assigned to one or many roles and each role can be assigned to more than one permission. And also, the Core RBAC possesses a set of sessions where each session has occurred by mapping between a user and a subset of role that is activated and assigned to the user. The following components contained in the definition of the Core RBAC model:

- USERS define the set of users, ROLES define The set of roles, Permissions define the set of permissions and SESSIONS define the set of sessions;
- PA: ROLES → Permissions, the function of the permission assignment that role is assigned permissions and the permissions is necessary to accomplish their job;
- UA: USERS → ROLES, the function of the user assignment that the users is assigned roles;
- User_sessions: USERS → SESSIONS, that a single user is assigned each session ;
- Session_roles: SESSIONS → 2^{Roles}, that each session is assigned the set of role.

B. Hierarchical RBAC

In Hierarchical RBAC, permissions of the role can be inherited from relationship among roles. Any combination of role hierarchy may optionally be included in a particular RBAC system. Inheritance has been described in terms of permissions; that is, senior role R1 inherits junior role R2 only if all permissions of junior role R2 are also permissions of senior role R1. Hierarchical RBAC introduces the concept of authorized user's role and authorized permissions and role hierarchies consist of two types: general role hierarchies and limited role hierarchies [2]. General role hierarchies support the concept of multiple inheritances which provides the ability to inherit permissions and to inherit membership of user among roles. Limited role hierarchies enforce restrictions which result in a simpler tree structure (i.e., a role may have more than one immediate ascendants, but is restricted to one immediate descendent) [1].

C. Constrained RBAC

Constrained RBAC is the combination of separation of duty to the hierarchical and core RBAC model. Separation of duty are applied to impose conflict policies that organizations may employ to protect users from committing fraud over a reasonable authority level for their responsibilities. Separation

of duty has long been recognized as a security principle for its wide application in bank, department and office. Constraints RBAC provide static separation of duty (SSD) and dynamic separation of duty (DSD). Static separation of duty (SSD) can apply to user-assignment (UA) relations that the roles are assigned to user. Dynamic separation of duty (DSD) can apply to Session-roles relations and permission-assignment (PA) relations. Separation of duty refers to the responsibilities of organization that associated with permissions among different roles.

SSD occur particular user that assigned to the role by replacing constraints on the users. SSD may exist within hierarchical RBAC. Membership of the same role cannot allow to be a member of one or many other roles. The inheritance of SSD constraints include in the hierarchies of role.

DSD can limit the accessibility of a user's permissions on permission space by setting constraints on the activated roles. DSD can also support for different permission levels of each user in the principle of least privilege at different times. This ensures that permissions do not carry on over the time that they are needed to perform task. Without the provision of dynamic separation of duty, permissions can be a complex issue.

IV. Proposed RBAC Learning Management System

Learning Management System (LMS) is progressed in the world of online learning as well as Web based application for communication, certificate of the learning programs, online examinations, training, forums and online competitions, e-learning programs. This proposed LMS can support the following functions:

- To perform registration and enrollment process for teachers and students.
- Create the different roles of users.
- Update courses in the LMS.
- Describe the timetable.
- Upload and download assignment and course

The users of proposed LMS are students, teachers and administrator.

LMS has been used to manage a large amount of data as a multi-user application. The benefits of LMS are easy to use great learning functions on the user-interface and web application can also be provided as the back-ground technologies. According to the properties of fundamental LMS, store of data can be retrieved easily without any access control but nowadays, many users require to access more than one permissions and enormous data in the multi-user web applications. This proposed system can handle multi-user simultaneously and can secure the data and information of LMS server. RBAC model is contributed to control the permissions over the secure data and manage to authorize users.

A. Proposed Role Based Access Control Model of LMS

Among a variety of RBAC model, this paper exploits especially the Core RBAC added with Dynamic separation of duty (DSD) mechanism applied in LMS. The purpose of this plan is to protect the unauthorized user and permission. Core RBAC combines with DSD model is most suitable for this system. The structure of RBAC combination model in LMS describes as follows:

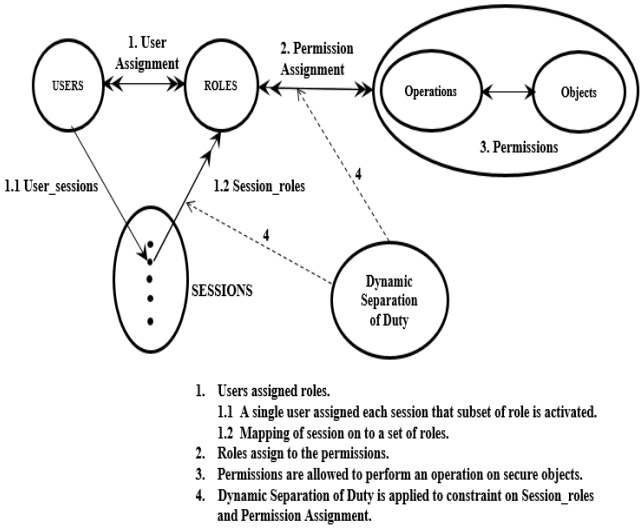

Fig.1.The structure of RBAC combination model in LMS

As show in figure (1): When the user start login to the system, the system establishes a session that is activated role to perform their permission. Each user can assign one or more roles and same role can be assigned many users. Furthermore, each role assigns many permissions and the same permissions can be related with many roles. The user accessible to the permissions that are assigned to the roles and currently can be activated across the user's sessions. If the system wants to restrict the permissions to any role, dynamic separation of duty (DSD) will be applied to permission of role that is activated within the user's session. (For example, the students are allowed to take their exams or quiz during the given period of time. Some of the permissions will be prohibited beyond the time that the users are required for performance of their duties.)

B. Proposed System Design of RBAC Learning Management System

For system security, this system must control the variety of users who operate their own authority on the object. Role based access control is essential for security aspect to provide insecure access to specific Web Service. In this system, the system administrator is responsible for creating roles that assign users and permissions to the system according to the level of users and their responsibility. The users (students, teacher and LMS admin) must have their own identities and passwords to authenticate during enter the system login after that they can perform their permissions in the system. The LMS admin can manage to user's (students or teachers) role.

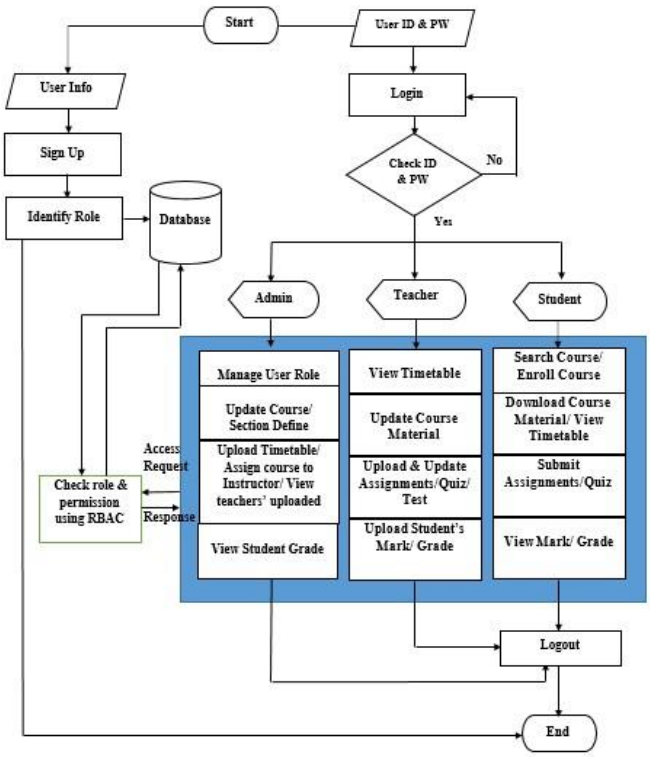

Fig.2. Role based access control in learning management system design

As show in figure (2): In this system, firstly the user must enter identity and password to request for LMS operation. If those authentication is OK with predefined role, LMS starts the operation and the system checks the RBAC permissions or privileges for that user who was specified in the page or user interface. After that server checks RBAC permissions or privileges for the user in LMS server and if those permissions are OK, the user can do access right that concerns with their permissions (for example: Read, write and execute are operated in the file system; Insert, delete, append and update are operated in the database management system) to LMS.

The traditional LMS applied access control list (ACL) method to ensure authentication for users and the proposed role based access control LMS applied the combinations of Core RBAC and Dynamic Separation of Duty RBAC model to secure data. According to the comparison of these two systems as shown in table (2), we can see that the proposed system is well secure against interfering and manipulation of data.

Table II. Comparison of Traditional LMS and Role Based Access Control LMS

Secure data process	**Expected Results**	
	Traditional LMS Results	***RBAC LMS Results***
Control the permissions over the secure data and manage to authorize users.	Unsolved	Solved
Prohibited beyond the time that the users are required for performance of their duties (Time control).	Unsolved	Solved
Provide exactly the right access, to the right user, at the right time	Unsolved	Solved

V. Conclusion

In this paper, RBAC feature is applied while implementing learning management system in order to protect the un-authorized user access. We believe that the proposed RBAC model can improve upgrade the security of learning management system.

By using Core RBAC in propose system, the user can be assigned many users-roles and simultaneously assigned permissions. Also we were able to apply our constraint on the users who attempt to access the data over the period of time by using dynamic separation of duty (DSD) on user's permission.

As the feature of proposed model, it is convenient for the system security and better access control capability, and perfectly protected to learning management system in security concerned.

ACKNOWLEDGMENT

I am highly thankful to Dr. Khine Moe Nwe for her active guidance and kindly comments throughout the completion of this paper.

References

[1] American National Standard for Information Technology "Role based access control," ANSI INCITS 359-2004.

[2] Dharmendra Choukse and Umesh Kumar Singh, "Role based access control with single sign-on architecture using web services for LMS," vol. 180, no.21, February 2018, pp. 25-30.

[3] Han Li Tin Win, "Simulation of role based access control in MySQL," University of Computer Studies Yangon in 2010.

[4] LIU Dongdong, XU Shiliang, ZHANG Yan, TAN Fuxiao, NIU Lei, ZHAO Jia, "Role based access control in educational administration system," ICMITE 2017.

[5] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein and Charles E. Youman, "Role based access control models," vol. 29, no. 2, February 1996, pp. 38-47.

[6] Muhammad Asif Habib and Christian Praher, "Object based dynamic separation of duty in RBAC" December 2009, pp. 512-516.

[7] Chia-Chu Chiang and Coskun Bayrak, "Modeling role based access control using a relational database tool," USA, August 2008, pp. 7-10.

[8] N. Li, Z. Bizri and M. V. Tripunitara, " On mutually exclusive role and separation of duty," October 2004, pp 42-51.

[9] Ravi S. Sandhu, "Role based access control," Advance in Computer, vol. 46, 1998, pp. 237-286.

[10] R. Sandhu, David F. Ferraiolo and David R. Kuhn, "The NIST model for role based access control: towards a unified standard" Berlin, July 26, 2000, pp. 47-63.

[11] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, David R. Kuhn and Ramaswamy Chandramouli, "Proposed NIST standard for role based access control," vol. 4, no.3, August 2001, pp. 224-272.

[12] Ankita Sharma and Dr.Sonia Vatta, "Role of learning management systems in education," vol. 3, Issue 6, June 2013.

[13] Joon S. Park, Gail-Joon Ahn and Ravi Sandhu, "Role based access control on the web using LDAP," vol. 87, 2002, pp. 19-30.

[14] Elisa Bertino, Piero Andrea Bonatti and Elena Ferrari, "TRBAC: a temporal role based access control model," vol. 4, no. 3, August 2001, pp. 191-223.

[15] Ankita and Dr.Sonia Vatta, "Role of learning management systems in education," vol. 3, issue 6, June 2013, pp. 997-1002.

[16] Alessandro Bozzon, Tereza Iofciu, Wolfgang Nejdl, Antonio Vineenzo, Taddeo and Sascha Tonnies, "Role based access control for the interaction with search engines," 2007.

[17] Ninghui Li, Ji-Won Byun, Elisa Bertino, “A critique of the ANSI standard on role based access control,” v ol. 5, no. 6, 2007.