Role - based Access Control in Educational Administration System

LIU Dongdong[1], XU Shiliang[1] ,ZHANG Yan[1] ,TAN Fuxiao[1],NIU Lei[1],ZHAO Jia[1]
[1] School of Computer and Information Engineering, Fuyang Normal University Fuyang, China

Abstract. In the 21st century, the network of teaching management not only improves its quality and efficiency but also brings convenience to teachers and students. However, as a network application system, it also faces a variety of security issues. In order to improve the system security , the widely-used RBAC control method is introduced in this paper. Based on the refinement of system privilege and user role, this paper puts forward the security management model of "user classification, role authorization , Unified management ", which is more suited to the structure of multi-level applications by controlling the data range accessible to users, and ultimately achieves the purpose of strengthening the security of the system.

1 Introduction

In the 21st century, along with the rapid development of computers and the widespread use of the network, the growing size of the school, are making the school's educational administration is extremely important, educational management network model not only to teachers and students to bring convenient But also improve the quality and efficiency of teaching management. Combine the characteristics of the current school development, make full use of the existing campus network resources, development in line with the future development of the school educational management system, and further optimize and improve educational management methods and processes for better teaching services, has important practical Meaning, but also can promote the school's information technology and digital campus construction. As an important subsystem of the digital campus, the educational administration system is also very important. In order to solve the traditional security problem in educational administration system, this paper puts forward the RBAC-based control method which is widely used in the system[1]. Through the refinement of system privilege and user role, the control data can be accessed, So that the model is more suitable for multi-level application structure. The paper puts forward the security management mode of "user classification, role authorization, unified management", and finally achieves the purpose of strengthening the security access of the system.

2 RBAC

Role-based access control (RBAC) is the role through the contact users and permissions, by directly to the role of authorization to control the ownership of the user's access to the system operation. What is "role", in fact, the user can operate in the system permissions set, the definition of the role, the system can give users different roles to obtain the appropriate access. Users have many-to-many relationships with roles, and roles and permissions are also many-to-many. This mechanism allows the user to have privileges only through the role. In the basic structure of RBAC, each user in the landing system will establish a session (Session), and through the session to activate the role of the user and activate the role contains all the privileges (as shown in Fig1). In the RBAC model, role can exist inheritance relationship, that is, upper level role can be part or all of the inheritance of the role of the next level of authority, this role inheritance relationship to form the role of the hierarchy.

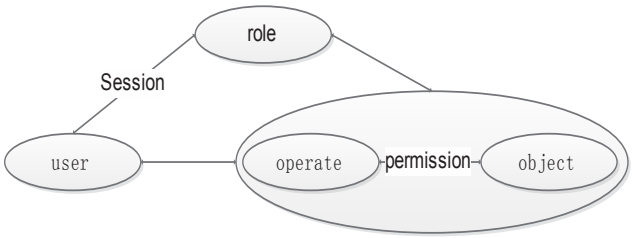

Fig1 Basic structure of RBAC

The hierarchical structure of the role can correspond to the hierarchical structure within the organization, the different roles corresponding to different functions or positions, which can be based on the user's position to grant the role. So that once the responsibility of the user position changes or add new applications in the system, the system as long as relatively simple to change the user's role, or in the role of adding new permissions to modify the user's permissions, in addition, you can revoke user roles Or role permissions.

3 System security analysis

The security scheme of the educational administration system is based on the role-based access control under the premise of identity authentication, so the system security requirements mainly involve the following aspects:

1) users and rights management

The system administrator is responsible for managing each user and authority in the system. Its specific management functions mainly include creating users and roles and defining and assigning various operation rights of the system, and according to the user's level and responsibility. Role of the grant and recycling, to ensure that each user can only be authorized within the scope of legitimate operations, while the system administrator also has the appropriate resources to manage the operation of the corresponding functional data responsibilities.

2) user authentication

School students, teachers and managers at all levels use their own account number (student number, employee number, etc.) for system login. Only users with identity and password authentication during logon can perform their own privileges in the system.

3) Access control

WEB server, database server are deployed in the campus network platform, the system must strictly control the various users can only perform their own operating authority to ensure system security.

3.1 User role analysis

RBAC model in the management of user rights is based on the role of the general role can be given to multiple users with a role, but also can give a variety of roles to a single user. Any user of a system has a unique symbol (UserID, user name, employee number, student number, etc.)[2] that can identify itself in the system. The user must first authenticate the identity through the authentication module when logging in the system. Of users can log on the system, and the system
also need to determine whether the user is already in the login state of the function, to prevent duplication of registration caused by various information fraud. The following are two requirements for the roles in the educational administration system:

1) The role of the educational administration system created by the administrator, specifically according to the school's organizational structure and the actual business functions set, the system provides a special module to manage users and roles.

2) Each role in the academic management system also has a unique number to identify their own, and save the role of the relevant institutional information (such as college, department number), which can facilitate the role and authority to manage.

3.2 Object privilege analysis

Objects in the system include the various visible objects in the system window, such as menus, buttons, etc., but also invisible objects in the database, such as records, fields, and so on. Educational Administration System itself consists of various functional modules and a variety of system window menu command together. Each user or role can have its own functional modules and menus, through the role and user authorization to achieve the control of the object operation. Specific practices are as follows:

1) the establishment of the role of the authority table,

in which the role of each role in the system records of the operation of the system resources. At the same time, this table also reflects the system's various business functions.

2) The module function of the system can be expressed in the form of the function menu, which can facilitate the control of users with certain roles to add, delete, change and so on the function modules in the system.

3) As the role of the size of the problem of partition, each role has a corresponding set of permissions, and when a user has more than one role, then the user should have access to all the roles of its authority is a role of authority And set, in this case, the union may appear duplication of the same user rights, but this does not affect the user has the total permissions.

4) The administrator in the user function module for the distribution of authority, the main strategy is to set the user in the function of the various components of the object permissions, such as menu, field properties.

In the basic structure of the RBAC model, the user will establish a session with the system upon login, which is responsible for activating all the roles granted by the user. The user can have the role of the authority during this session, the user during the establishment of the process of access to the system role of the specific process as shown in Fig2.

After the user logs in to the system and the authentication succeeds, the user obtains the role and the corresponding authority, and determines whether to allow the access request resource according to the role privilege[3]. Fig5 is a state diagram of the user login system, reflecting the process of user login system status.The security scheme of the educational administration system is role-based access control under the premise of identity authentication, so only the users who succeed in authentication can have the role privilege and access the corresponding system resources. The authentication function of the educational administration system is realized by Java security programming interface The certification process is roughly described as follows:

When the user logs in, the system creates the LoginContext object. The LoginContext object is then used to query the configuration file login.config, and the LoginModule object is loaded according to the configuration file. The user is authenticated by running login () and the CallbackHandle object is created at the same time..

Principal is used to represent the user's access rights, thus completing the verification step.Fig3 shows how the authentication framework processes the Web page request.

4 RBAC-based access control model design

4.1 Design of role privilege management scheme

In the overall scheme of access control, granting and reclaiming various rights is the key point of the authorization process, and in order to increase the security and flexibility, we

plan to manage the role categories and functions independently. According to the specific situation of the school, the specific plan of RBAC in the educational administration system is to classify the school personnel, to determine various roles, to restrict role based on role, and to unify management roles and rights: "user classification, role authorization and unified management".

1) Role definition

Due to the fact that there are a lot of users in academic institutions and the different levels of identities, levels and levels in the secondary school, there are many types of roles that need to be divided in the system. Often, Of the staff will have a lower level of operational authority, so the system through the introduction of inheritance between different roles to reflect the relationship between the different levels of human rights include (for example: in charge of teaching authority will include teaching in charge of two Level role of the Dean of the authority), role inheritance is the use of object-oriented programming thinking inheritance between the characteristics of the specific approach is to expand and classify existing roles to derive new roles, the benefits of doing so is to avoid duplication of definition, This is in line with the teaching management in the flexible management and level management.

2) permission to configure

In RBAC, the role is essentially a user collection,

and because the permissions are granted roles, so the role is the permission set. And can grant a user multiple roles, but also can grant a role more than one authority, of course, can also grant a role to more than one role. Permission configuration is actually the role of configuration permissions, because only the role has permissions, can be granted to the user through the role.

- Divide staff roles

In the educational administration system, it is the main core idea of RBAC that authority and user are connected by role. In view of the division of personnel roles, this paper takes the design idea as follows: starting from the specific needs, analyzing all kinds of personnel roles in the school, on the basis of the division and division of good user roles, and then the role of classification, and finally assigned to the hierarchical authority Character.

In fact, in any unit, people or positions are divided into different levels of hierarchy, different positions have different roles, and therefore have different permissions. Although different positions are not exactly the same as the role of division, but the role of the system as the level of distinction between the level of the same job[4]. For example, in the system, in charge of teaching school principals and system administrators, the role of the system administrator is actually more important than the principal, so the system administrator should have greater system privileges, which in the role of the division to reflect the different Level of the hierarchy.

In the school, the general use of educational administration system users mainly include: system administrators, departmental administrators, module administrators, teaching management personnel and a series of management personnel and general teachers and students. When we divide roles into these users, the strategy is to first split the roles into two different levels:

1)low-level roles both general role: including ordinary teachers and students, the role of the class have some common ground: the authority is generally fixed limited, in the role of such authorization, the general can be granted directly to the fixed authority .

2)senior roles both special roles, including system administrators, module administrators and various types of teaching administrators, the role of the general level of ownership of more authority in the role of such authority may be granted directly, but also Granting other roles, that is to say other roles become their sub-roles, so that sub-role can be granted through the indirect grant. For example, in charge of teaching the role of school principals and in charge of the teaching of the secondary college dean role is clearly a role in the inheritance relationship. Fig4 is the role of educational management system in two types of division.

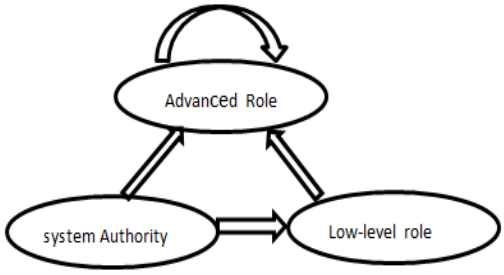

Fig 4 Two types of role classifications

As you know, a privilege can be granted both a high-level role and a low-level role, but there are differences between the two types of roles in granting permissions: the lower-level role can be granted directly, and the higher-level role can Inheritance of low-level role or other high-level roles, the role of the parent role of the inheritance of sub-role, the role of the high-level authorization is more flexible, in addition to its authority can be granted directly, but also inherit other roles permissions.[5]

Follow the above rules to classify and classify the various roles of the educational administration system (low-level role, senior role), the specific division is as follows:

1) Low-level role: students, general teachers, counselors.

2) senior role: Senate Secretary, Department (College) administrator, school leadership, super administrator.

- Assign system privileges

RBAC design program includes two key technologies: one is the role, we have previously described the division and hierarchical roles; the other is the permissions, and role similar to the authority also need to divide the RBAC RBAC management system in this paper design, The plan divides authority into three

categories[6]:

1) Departmental authority: This kind of authority generally belongs to the departmental role. For example, the academic secretary of the School of Economics and Management only has the authority of the college's resources in the operating system, and can not operate the resources of other colleges.

2) Function Permission: This kind of authority decides which system function module the user can use and can not use which function module.

3) data permissions: This type of permissions are mainly used to limit the operation of the data in the database, used to determine the different data objects (data tables, views, etc.) for what the permissions (search, entry, change, delete, etc.) .

The above types of permissions through the role of the system with the operating system resources to limit access to the purpose of protecting the security of the system. In the specific application, in the role of grant permissions often need to combine three types of permissions, therefore, the division of authority requires fine-grained division.

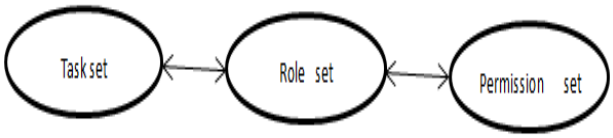

Fig 5 System authority division

Fig5 depicts the division of authority in the educational administration system, explained as follows:

1) Task Set: task division is actually the decomposition of the system functions, and function refers to the need to perform the task, task set is a collection of all functional tasks.

2) Role set: the role corresponds to the number of tasks to perform, so according to the task set the role, and the permissions are granted to the role. A character set refers to a collection of roles.

3) permission set: role with the system permissions are determined by the role of the corresponding set of tasks, the role of the corresponding set of permissions on the various modules of the call.

4.2 Model structure design

Due to the large number of staff, the number of users who use the educational administration system at the same time is also very large. . In order to ensure the security of educational administration system, it is very important to design a set of secure and flexible security access control module. Based on the traditional RBAC model, this module introduces the security principle of separation of users and responsibilities, Authorization, unified management "objectives, the design of educational administration management system security access control model structure shown in

Therefore, the security management system is composed of two parts: identity authentication controller and access controller. Among them, the premise is the identity authentication controller, the core is the access control server, access control server consists of four parts: the user role server, role permissions server, permissions library, and the role of libraries.

5 Summary

In the educational administration system, we introduce the commonly used relatively secure and flexible role-based access control strategy, and RBAC model in the role and permissions to be graded and refined, and the design of the
RBAC model program applied in the educational administration system. From the actual results, this RBAC program can meet the system security requirements, and has better control access capability, and effectively protect the educational administration system in operation security.

ACKNOWLEDGE

This work was supported by the following project:
(1) National Natural Science oundation(61673117,61401101)
(2) Natural Science Foundation of Anhui Provincial Education Department(KJ2016A551, KJ2016A549,KJ2015A295, 2015KJ014,2015KJ007)
(3) National College Students' innovative projects (201610371028, 201610371029)

(4)Fuyang Normal University Foundation
(2013ZYSD05,2013KJFH05,2013FSKJ14,2015KJFH02,
2015FSKJ09, 2016PPJY30, rcxm201710)
(5)Anhui Province Quality Project(2014zdjy083,
2014zdjy080,2014zy048)

. Reference

[1] Jia, Z., Pang, L., Luo, S. S., Zhang, J. Y., & Xin, Y.. A privacy-preserving access control protocol for database as a service. In2012 International Conference on Computer Science & Service System (CSSS) (pp. 849–854). IEEE. (2012)

[2] Jia, Z., Pang, L., Luo, S. S., Zhang, J. Y., & Xin, Y.. A privacy-preserving access control protocol for database as a service. In2012 International Conference on Computer Science & Service System (CSSS) (pp. 849–854). IEEE. (2012)

[3] Yaish, H., & Goyal, M. Multi-tenant database access control. In2013 IEEE 16th International Conference on Computational Science and Engineering (CSE) (pp. 870–877). IEEE. (2013)

[4] Xinchao Song, Yishuang Geng, Distributed community detection optimization algorithm for complex networks, Journal of Networks, 9(10), 2758-2765, Jan. (2014)

[5] Jiang D, Ying X, Han Y. Collaborative multi-hop routing in cognitive wireless networks[J]. Wireless Personal Communications: 1-23. (2015)

[6] Yaish, H., Goyal, M., & Feuerlicht, G. An elastic multi-tenant database schema for software as a service. In IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (Dasc), 2011 (pp. 737–743). IEEE.(2011)

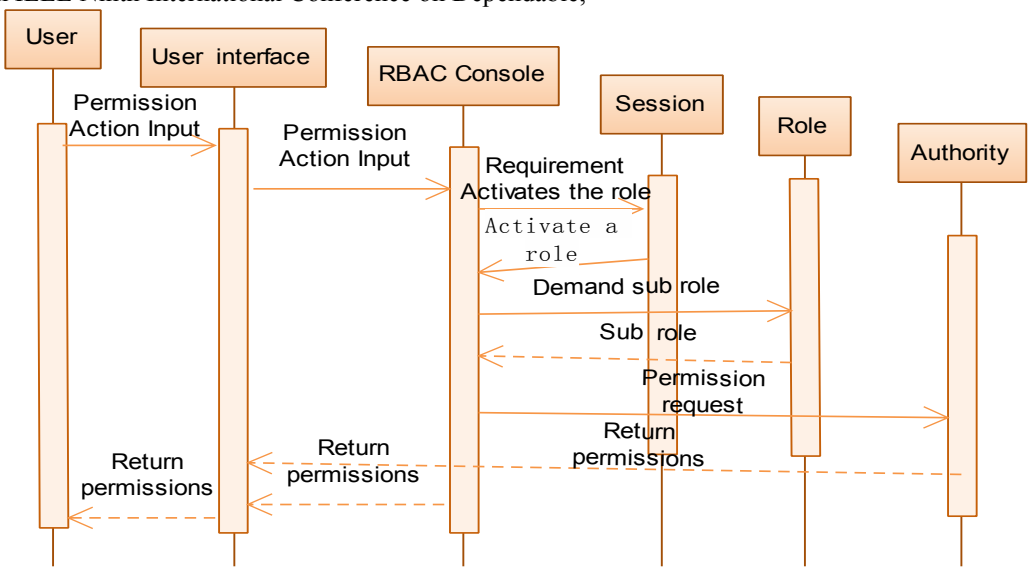

Fig 2 Collaboration diagram of the RBAC session

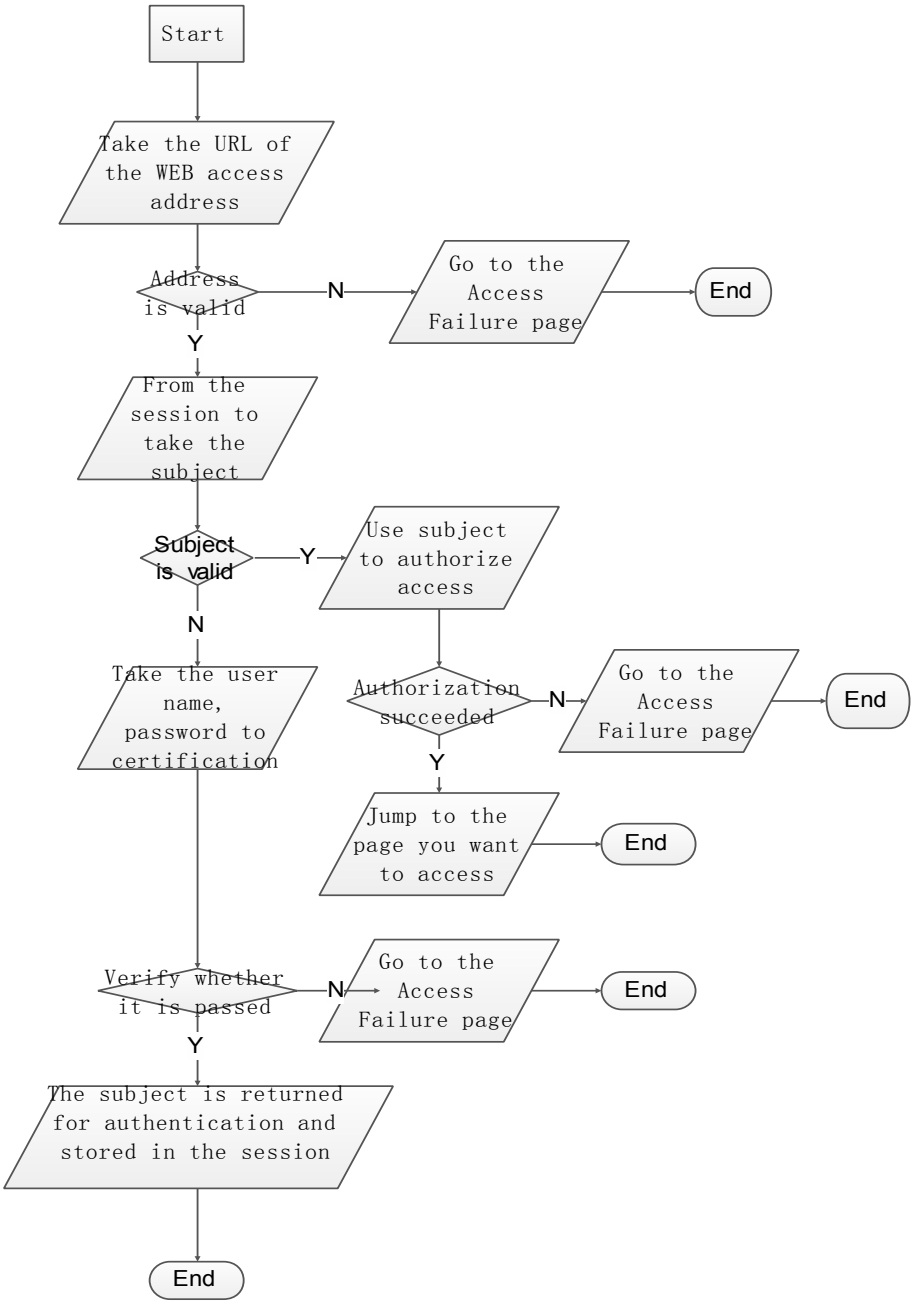

Fig 3 Authentication framework to handle WEB page requests

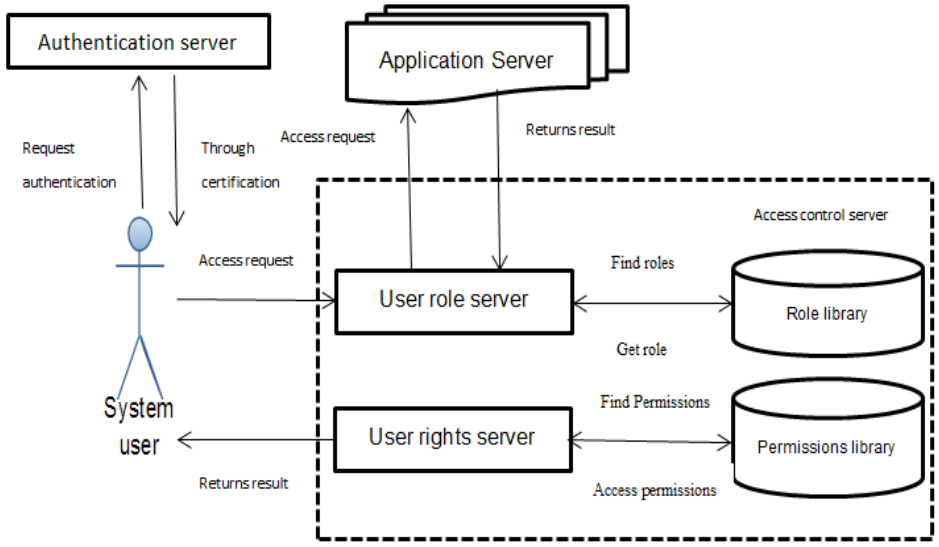

Fig6 Role-based access control system architecture