Access control method of multimedia distance education resource database based on Web Platform

LIANG Yan[1], WANG Fei-fei[2]

{LiangYan3263@163.com[1], WANGfeiF06@163.com[2]}

[1,2]Jilin International Studies University, Changchun 130000, China;

Abstract. In view of the shortcomings of the traditional access control method of multimedia distance education resource database, which is slow to access due to the poor control effect, this paper proposes a web-based access control method of multimedia distance education resource database. According to the web platform to establish access control model, on this basis, through the role division, user management, role management, authority management, user role assignment management and role authority assignment management, the design of access control method of multimedia distance education resource database based on Web platform has been completed. Through the comparative experiment, compared with the traditional access control method of multimedia distance education resource database, the experimental results show that the access speed of the proposed access control method of multimedia distance education resource database based on Web platform is faster.

Keywords: Web platform; Database; Access control;

1 Introduction

With the development of Internet, resource sharing becomes more and more simple, and resource sharing platforms emerge in endlessly. However, the database security problems brought by resource sharing for resource sharing platform are increasingly serious. Access control technology is an effective way to protect database resources [1-3]. Multimedia distance education resource database is a typical resource sharing platform. The access control of database can restrict the access ability of users, and effectively prevent the invasion of illegal users or the misoperation of legitimate users from bringing adverse consequences to the database [4-6]. Security research has always been a hot topic in the field of computer science and technology. Most scholars focus on how to improve and optimize the authorization access control strategy, for example, from the traditional access control such as independent access control DAC and mandatory access control MAC to role-based access control strategy

EAI MOBIMEDIA 2020, August 27-28, Harbin, People's Republic of China

DOI 10.4108/eai.27-8-2020.2294588

(RBAC). The current authorization access control can be roughly divided into two categories: database level security management, such as operating database level security management, database level security management, etc.; the other is application level security management, which mainly depends on the specific database [7]. Such authorization access control module is usually composed of user authorization database or data file, user authentication and authorization hard coding in application database. Every time a new application is established, the authorization access control part has to be redesigned; such mechanism is not conducive to the control under distributed environment, reduces the efficiency of application database design and development and database compatibility Sex and expansibility.

The rapid development of network technology has given birth to new network applications. Web based applications and clients are penetrating into traditional desktop applications. The increasingly rich network applications have put forward new challenges and requirements to the security control technology. At the same time, with the rapid development of Web services technology, software tends to exist in the form of services. Authorized access control technology based on Web Services provides a new idea for security design. Web service is recognized as an advantage technology to solve the integration of heterogeneous databases in the network environment. It provides good integration performance of heterogeneous database and cross platform. On this basis, combined with RBAC and web services technology, the access control method of multimedia distance learning resource base based on Web platform is designed. This method makes the authorized access control module easier to adapt to the security requirements of heterogeneous database, and easier to configure and maintain.

2 Access Control Method of Multimedia Remote Teaching Resource Database Based on Web Platform

2.1 Establish access control model

Based on the web platform, RBAC (role-based access control) is introduced into the concept of grouping to realize active authorization. It is not like RBAC, users can have access control rights to resources after granting roles to users, nor simply allow users belonging to a certain group to have full control over resources of their own group, but group them according to colleges and universities. Because resources and users of multimedia remote teaching resource database are from colleges and Universities, when colleges and universities are

grouped, the number of The database also groups users [8]. When permissions are assigned to the role, the permissions of users in this role will be limited to the group in which they belong, and the access to resources by users will be limited to the resources in this group.

The user permission information in the group and role-based access control model will be transferred through sessions. There are three kinds of sets in the model: user set u, role set R and group set G, as shown in Figure 1.

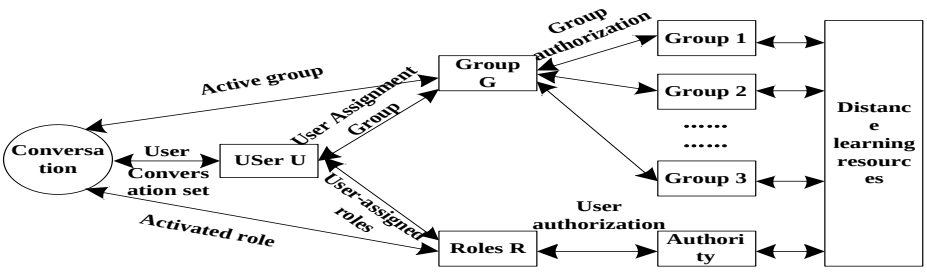

Fig. 1. Access Control Model Diagram Based on Grouping and Role

When the user is authorized to enter the database, the information interaction between the session and the user u is carried out through the user session set. The grouping and role information of the active user stored in the session set are the activated grouping and role information, and the authority judgment can be effectively carried out in the database [9]. The group assignment between the group information of user u and group G uniquely determines the scope of user activity. The role assignment existing between the role information of user u and role r uniquely determines the user operation permission. Users authorized by groups and roles access resources, that is, access resources within their scope of activity according to their own permissions.

First, in the model, we build the relationship among groups, roles and users. According to the above-mentioned access control model based on grouping and role, combined with the actual situation of multimedia distance education resource database, the designed relationship between grouping, role and user is listed as follows. Because grouping is based on colleges or units, it also involves the subordination relationship between grouping and colleges. The database has four roles: database administrator, general administrator, teacher and student; each group has three roles: general administrator, teacher and student; the database administrator does not belong to any group (it can also be considered that the database

administrator belongs to all groups), the management group can be added and deleted, and any information (user information, courseware information) of any group can be seen Information, courseware entity, resource statistics query report, etc.); Roles and users are one to many relationships. A user can only have one role, but a role can correspond to multiple users. After users register, they are assigned roles first, and then assigned groups; each user's corresponding roles and groups are one to one relationships; groups and colleges are one to many relationships, and each group has one or more colleges or units, one to many relationships After a user belongs to a certain group, one or more institutions or units in the group should be redistributed. Ordinary administrators and teachers can assign one or more institutions under their jurisdiction; students can only assign one institution; Therefore, the relationship between users and institutions can be divided into two types according to different roles: the relationship between ordinary administrators and teachers and institutions is one to many; the relationship between students and institutions is one to one.

Secondly, in the model, the user status is designed as follows: the huge user group will inevitably bring the complexity of user account management. Even if the access control of users is limited by groups and roles, it can not guarantee to find and solve problems in time when the database is running.

In the design of access control system, after user authentication and before authority judgment, the management of user status is added to enhance database security. Users can have three statuses in the database: the pending status of newly registered users, the enabled status with legal permissions, and the disabled status caused by illegal or misoperation. In the design of user status, setting all newly registered users does not immediately have access to the database, but needs to pass the administrator's audit. The administrator views the user information in detail during the audit process to ensure that the user is trustworthy in the database. At the same time, the administrator can also adjust the user's grouping and role information to assign reasonable rights to the user the limit is [10]. When users pass the audit, they can become legal users of the database. If the user's behavior in the database endangers the database security or information security, resulting in database exceptions, the administrator can immediately freeze the user's access rights by disabling the account, and retain the user's information in the database, and re enable it after eliminating the user's threat. The function of user status is embodied by storing the corresponding status fields in the

database. Therefore, the basic identity information of each user logging in the database, in addition to his / her user ID, password, has his / her user status word.

Finally, in the model, the permission string is designed as follows: throughout the permission management of the whole database, due to the complexity of resources and user information, plus retrieval, statistics and other resource services, if users are grouped and divided into roles, more permission points need to be controlled. If the database users are grouped or the role changes, it will inevitably cause a lot of changes in permission points, and the frequent setting of permission system will have a lot of work. Therefore, in the design of user management module of the database, all the parts that need to be controlled by permission will be summarized and listed one by one in the way of permission limit points. In the database, the method of permission string is used, and "1" is used to represent With this permission, "0" means no permission, and a string corresponds to the permission range of a role to simplify the permission control process. As shown in Figure 2, it means that the user can browse resources, view resource statistics results, retrieve resources, download resources and publish feedback on resources.

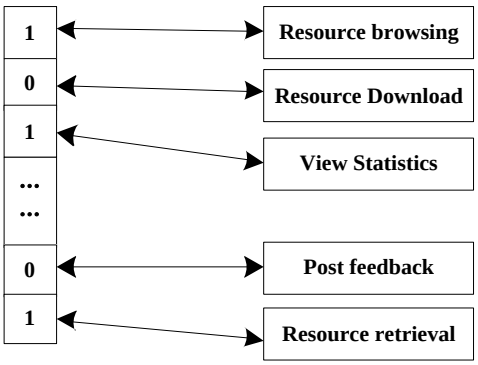

Fig. 2. Permission string diagram

The permission corresponding to each function page of the database will occupy one of the permission strings. When a user accesses the page, he can determine whether to allow the user to access the resource by reading the character bit of the page corresponding to the permission string in the user session information as 1 or 0. 1 indicates the legal user, and 0 indicates the illegal access. The emergence of the permission string also provides great

convenience for the role to assign permissions. The database administrator only needs to select the corresponding string for each role on the permission string setting page to complete the authorization of the role, which greatly simplifies the authorization process. Due to the existence of user groups, the assigned permission string can only take effect within the scope of the group to which the user belongs. Administrators don't need to worry about group access of users after permission assignment. After the establishment of the model, based on the web platform, the access to the multimedia remote teaching resource database is controlled, and the specific content is described as follows.

2.2 Role division control

Role classification is only a general division of roles, any information processing database is to complete certain task functions, so any role should be set according to the specific task requirements of the database, and the role should always perform certain tasks in the database. For this purpose, symbols are introduced to represent: $A=\{a_1,a_2,\cdots,a_n\}$ role set. Among them, a_n is the specific role of multimedia distance education resource database. $T=\{t_1,t_2,\cdots,t_n\}$ task set. Among them, t_n represents a specific task in the database. Task set for role $A^T \subseteq 2^T$. In the multimedia distance education resource database, t_i represents the entry of multimedia distance education resource item, t_j represents the modification of multimedia distance education item, and t_k represents the audit of database. If $r_i^T=\{t_i,t_j\}$, it means that r_i is the role of resource recorder in the multimedia distance education resource database; if $r_j^T=\{t_k\}$, it means that r_j is the role of resource auditor in the multimedia distance education resource database. The new role is added to the database by using the addrole (role) algorithm. The premise is that there are no new roles in the current role set. Enter the name of the newly added role; if the role is added successfully, the role ID will be returned; otherwise, null will be returned.

The specific implementation process is as follows:

Step 1: if there is a role with the same name as the newly added role in the current role set, you will be prompted "role already exists" and null will be returned, otherwise continue;

Step 2: add a new role in the current role set;

Step 3: update role information table rolelnfo, that is, add related records in role information. Roleinfo;

Step 4: return the system generated role ID.

2.3 User management control

The users of the multimedia remote teaching resource database based on the web platform are registered through the network registration. The user objects are teachers, students, educational administrators, school administrators, teaching and scientific researchers and other different categories, which are filled in by the user when registering. The user classification actually belongs to the basic role type in the system. The filling in of user registration application is only the basis for the system to assign roles, which does not mean that users automatically have roles. Users should also fill in the name, gender, unit, discipline and other information when registering. The purpose of the system background user management module is to manage the user's content and design the user's add, delete, modify and other operations. The trust value of the user is calculated by formula (1):

$$\mathrm{TrV}=\mathrm{initTrV}+\frac{\alpha * N_{OB}+(-\beta) N_{RB}+(-\gamma) * N_{DB}}{N_{OB}+N_{RB}+N_{DB}} \quad (1)$$

In formula (1), TrV represents the user's trust value, $\mathrm{initTrV}$ represents the user's initial trust value, α, β and γ represent the trust evaluation weight, and N_{OB}, N_{RB} and N_{DB} represent the total number of user behavior records with the behavior modes of OB, RB and DB respectively. The control of user management is realized through the following steps.

Add user (user) algorithm is used to control user add operation. If there is no new user in the current user set, add a new user to the multimedia remote education resource database,

enter the new user name user; if the user is added successfully, the user ID will be returned, otherwise null will be returned.

The specific steps are as follows:

Step 1: if there is a user with the same name as the newly added user in the current user set, a prompt "user already exists" will be prompted, and null will be returned, otherwise continue;

Step 2: add new users to the current user set;

Step 3: update user information table userinfo, i.e. add relevant records in user information table userlnf o;

Step 4: new users are mapped to empty sessions;

Step 5: return the system generated user ID.

The user addition in this database is added to the user information table userinfo after the user registration.

The deieteuse (user) algorithm is used to control user deletion. The premise is that the user to be deleted must belong to the current user set, and a user is deleted from RBAC system. Enter the name of the user to be deleted user; the output user deletion success returns true, otherwise returns false. The specific implementation steps are as follows:

Step 1: if there is no user to be deleted in the current user set, the prompt "user does not exist" will be prompted, and return false, otherwise continue;

Step 2: if the user is associated with an active session, delete the session (force close or exit)

Step 3: update the user assignment relationship (UA), delete all user assignment relationships of roles, that is, delete the user role assignment information table userroleinf. Relevant records in;

Step 4: delete the user from the current user set;

Step 5: update user information table userinfo, that is, delete relevant records in user information table userinfo;

Step 6: returns true.

Deleting a user usually includes the following situations: the user logs off actively, the user is forced to log off due to illegal operations, and the user is automatically deleted if he / she does not log on to the system within 90 consecutive days.

2.4 Role management control

The role of multimedia remote teaching resource database includes two basic role types: teacher and student. By inheriting the role of teacher, we can further divide the role types, such as education administrator, resource auditor, school administrator and teaching and scientific research personnel. These different roles have different permission sets. They have the rights to add, delete and modify roles. The content of roles in the database will change with the actual situation. Therefore, the purpose of role management module is to manage the content of roles and adjust the role information of users in time. Therefore, the operation of adding, deleting and modifying user roles is designed.

Using addrole (role) algorithm to control role management operation. If there is no new role in the current role set, add the new role to the multimedia remote education resource database, input the name of the new role, and output the role ID if the role is added successfully, otherwise null will be returned. The specific implementation process is as follows:

Step 1: if there is a role with the same name as the newly added role in the current role set, a prompt "role already exists" will be given, and null will be returned, otherwise continue;

Step 2: add a new role in the current role set;

Step 3: update role information table rolelnfo, that is, add related records in role information table roleinfo;

Step 4: return the system generated role ID.

Use the deleterole (role) algorithm to delete the role (provided that the role to be deleted must belong to the current role set). Enter the name of the role to be deleted. If the output role is deleted successfully, return true, otherwise return false. The specific process is as follows:

Step 1: if there is no role to be deleted in the current role set, it will prompt "role does not exist", and return false, otherwise continue;

Step 2: if the role is associated with an active session, delete the session (force close or close after exit);

Step 3: update the user assignment relationship (UA), delete all user assignment relationships of roles, that is, delete the relevant records in the user role assignment information table userroie;

Step 4: update the permission assignment relationship (PA) and delete all the permission assignment relationships of the role, that is, delete the relevant records in the role permission assignment information table rolepermissioninfo;

Step 5: update rolelnfo, i.e. delete relevant records in rolelnfo;

Step 6: delete the role from the current role set;

Step 7: returns true.

2.5 Authority Management Control

The purpose is to manage the content of authority, that is, to manage the operation of object objects, such as the addition, deletion and modification of authority. The following is a list of some algorithms that implement permission operations in the permission management module.

Use registerpermission to control permissions. For the registered legal permission (associate the resource object with the corresponding operation), the precondition is that the new operation is not associated with the object and the object supports the current operation. Enter the object resource object name and operation name operation. If the output registration succeeds, the permission ID will be returned. Otherwise, null will be returned. The specific implementation steps are as follows:

Step 1: if the precondition is met or not, return false, otherwise continue;

Step 2: whether there is an object in the current object object set. If there is no object, execute addObject (object) and continue;

Step 3: add the current operation item in the object ACL, and the new item is not associated with any role;

Step 4: return the system generated permission ID.

Unregisterpermission (object, operation) algorithm is used to deregister the specified permission, provided that the operation to be deleted has been associated with the object.

Input object resource object name and operation name operation; output logoff success returns true, otherwise false. The specific implementation process is as follows:

Step 1: if the precondition is met or not, return false, otherwise continue;

Step 2: delete all related operation items in the ACL of the specified object;

Step 3: returns true.

2.6 User - Role Assignment Management Control

User role assignment management is mainly based on the functional requirements of the user role assignment information table userpermissionlnfo for related operations.

The assignuser (user, role) algorithm is used to assign a role to a user, provided that the user belongs to the current user set, the role belongs to the current role set, and there is no assignment relationship between the user and the role. Enter the user name and role name role; if the output assignment succeeds, true will be returned; otherwise, false will be returned. The specific implementation process is as follows:

Step 1: if the precondition is met or not, return false, otherwise continue;

Step 2: update the user assignment relationship (UA) and add the user assignment relationship of the role, that is, add the relevant records in the user role assignment information table userrolelnfo;

Step 3: returns true.

Use the deassignuser (user, role) algorithm to cancel the user to role assignment. The premise is that the user belongs to the current user set, the role belongs to the current role set, and the user and the role have an allocation relationship. Enter the user name use and role

name role; the output returns true if the assignment is cancelled successfully, otherwise false. The specific implementation process is as follows:

Step 1: whether the preconditions are met or not. If not, return false. Otherwise, continue;

Step 2: if the user and role are associated in an active session, delete the session (force close or close after exit);

Step 3: update the user assignment relationship (UA), delete the user assignment relationship of the role, that is, delete the relevant records in the user role assignment information table userroleinfo;

Step 4: returns true.

The user subset of the current role is obtained by using the assigned use: (role) algorithm. If the role belongs to the current role set, enter the role name role and output all user sets assigned to the specified role. The specific implementation process is as follows:

Step 1: whether the preconditions are met or not, if not, return null, otherwise continue;

Step 2: all users assigned to the specified role form a set;

Step 3: returns a pointer to hold the collection.

We use the assigned roles (user) algorithm to get a subset of the roles assigned by the current user, provided that the user belongs to the current user set. Enter the user name user, and output all the role collections assigned to the specified user. The specific implementation process is as follows:

Step 1: whether the preconditions are met or not, if not, return null, otherwise continue;

Step 2: all roles assigned to the specified user form a set;

Step 3: returns a pointer to hold the collection.

2.7 Role - Authority Assignment Management Control

The grant permission (permission, role) algorithm is used to assign permissions to roles. The precondition is that the execution role belongs to the current role set and the permission belongs to legal permission. Enter the permission name, authorization role name and role; if

the output assignment succeeds, true will be returned; otherwise, false will be returned. The specific implementation process is as follows:

Step 1: if the precondition is met or not, return false, otherwise continue;

Step 2: update the permission assignment relationship (PA), and add a new permission assignment relationship to the role, that is, in the role permission assignment information table rolepermissionif. Add relevant records in;

Step 3: returns true.

Revokepermission (permission, role) algorithm is used to revoke the relevant permissions assigned to the role, provided that the executing role belongs to the current role set and the permissions have been assigned to the specified role. Enter the permission name to be revoked, and the authorization role name role; if the revocation is successful, true will be returned; otherwise, false will be returned. The specific implementation process is as follows:

Step 1: if the precondition is met or not, return false, otherwise continue;

Step 2: update the permission assignment relationship ((PA), and add a new permission assignment relationship for the role, that is, in the role permission assignment information table rolepermissionif. Delete relevant records in;

Step 3: returns true.

Through the above content, based on the web platform, the access control of multimedia remote teaching resource database is realized.

3 Experiment

In order to verify whether the proposed control method has better control effect (faster access speed), a web-based access control method for multimedia distance education resource database is used.

3.1 Experimental process

First, the access control method is tested. The test environment is shown in Table 1.

Table 1 Test environment

Types of section	Hardware environment	Software Environment
Client computer	Windows XP Internet Explorer5.0 and above	CPU2.0GHz 256MB memory
Server computer	CPU 2.4GHz 1GB memory	Microsoft SQL Server 2005 IIS 6.0

In the above experimental environment, the access control method is tested. To test the logical relationship, we only need to test the functional logic of each module in the database which needs access control. Take the user status test as an example. There are three user statuses: enabled, disabled, and to be approved, corresponding to the status words "1", "1", "0".

The test process of user status is as follows. In each step of the process, you need to check the field changes of the test user's status word in the data table to complete the test of user status.

1. Register new user, expected status word: 0;

2. Audit the user as administrator "failed", expected status word: 0;

3. Approve the user as an administrator with expected status word: 1;

4. Modify the user grouping information as the user, expected status word: - 1;

5. Confirm the group information modified by the user as an administrator. The expected status word is: 1;

6. Delete the user's group as administrator, expected status word: - 1;

7. Re select the group as administrator for the user, expected status word: 1;

8. The user is actively disabled as an administrator, with the expected status word: - 1;

9. Log off the user as the user, and the user no longer exists.

After testing, the user status word will switch between "1", "- 1" and "0" according to the operation of each step in the process, and meet the expected results. All the user status functions are realized. The modules of input authentication, user login, user registration, user audit, user modification, user status, my resources, user deletion, group management, role management, resource access are tested. In the test process, combine the design and implementation conditions to design various use cases for various possible permission exceptions. Repeat each test case for 2-3 times. If each test result is the same and meets the expected result, the realization of this function meets the design requirements. Otherwise, it cannot pass the test and does not meet the design requirements. At this time, the program shall be modified and tested again Try until the design requirements are met. After that, the paper compares the speed of access under the control of web-based access control method and traditional access control method.

3.2 Analysis of experimental results

The comparison results of database access speed under the control of web platform based multimedia distance education resource database access control method, traditional multimedia distance education resource database access control method 1 and traditional multimedia distance education resource database access control method 2 are shown in Figure 3.

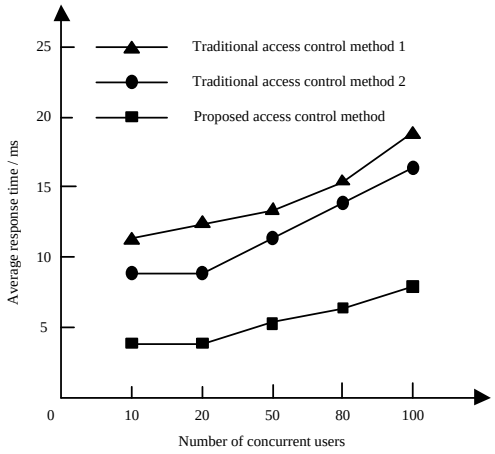

Fig. 3. Access speed comparison results

As shown in Figure 3, the average response time of the three access control methods increases with the number of concurrent access users. Among them, the average response time of traditional access control method 1 can be as long as 20ms when the number of concurrent access users is different; the average response time of traditional access control method 2 can be as long as 16ms when the number of concurrent access users is different; and the average response time of the proposed access control method is as short as 7ms. Through the analysis, it is found that the proposed access control method is based on the web platform, which greatly reduces the average response time and significantly improves the access speed.

4 Concluding remarks

In view of the shortcomings of the traditional access control method of multimedia distance education resource database, which is caused by the poor control effect and slow access speed, this paper proposes a web-based access control method of multimedia distance education resource database. Through the comparative experiment, compared with the traditional access control method of multimedia distance education resource database, the experimental results show that the access speed under the control of the proposed control method is faster, hoping that it can provide a certain reference value for the research of access control of multimedia distance education resource database.

5 Fund projects

This article is the phased research result of the demonstration virtual simulation experiment teaching project “Business Interdisciplinary Virtual Simulation Training” of Universities in Jilin Province (NO: JI JIAO GAO [2019]8)

References

[1] LU Xiao, BAO Xiaomin, RAO Zhaoming. Data Recording and Database Access Technology Based on LabView. Journal of Hubei University for Nationalities（Natural Sciences Edition）, Vol. 37, no. 2, pp. 201-205 (2019)

[2] YANG Ruijun, ZHU Ke, CHENG Yan. Database-level Web Cache Replacement Strategy Based on SVM Access Prediction Mechanism. Computer Science , Vol. 46, no. 6, pp. 201-205 (2019)

[3] LI Mingfei. Multi-channel Access Control Simulation of Self-organizing Network Based on Blockchain. Computer Simulation, Vol. 36, no. 5, pp. 480-483 (2019)

[4] WANG Ming, TIAN Mao, ZHAO Xin, et al. Research and Realization of Data Migration Tool Based on Hadoop Platform. Computer Measurement & Control , Vol. 26, no. 4, pp. 225-230 (2018)

[5] LI Huaiming, SONG Fangfang, WANG Lianqing. Research on Four Layer Access Control Model Based on Time and Environment Constraints. Computer Applications and Software, Vol. 35, no. 1, pp. 59-64 (2018)

[6] LEI Linan, LI Yong. CP-ABE based data access control scheme with multi-authorities. Application Research of Computers, Vol. 35, no. 1, pp. 248-252,276 (2018)

[7] ZHANG Yanhong, TANG Wei, YANG Binghua. Design and Practice of Online Teaching Supervision Based on Distance Open Education Teaching Platform: A Case Study of the Whole Network Teaching Platform of Yunnan Open University. Journal of YunNan Open University, Vol. 21, no. 2, pp. 81-86 (2019)

[8] GU Lifen. Research on CAPP System of Tractor Parts——Based on MySQL Database and Web Technology. Journal of Agricultural Mechanization Research, Vol. 40, no. 6, pp. 257-260,268 (2018)

[9] ZHANG Bin. Application of Unbalanced Data Mining in Distributed Database System. Control Engineering of China, Vol. 25, no. 7, pp. 1179-1183 (2018)

[10] YANG Jingping, GAO Lingling, FENG Ying. Bibliometrical analysis of research papers on adverse nursing events according to the Web of Science database. Chinese Clinical Nursing, Vol. 11, no. 2, pp. 123-126,129 (2019)