ISSN : 0974 - 7435 Volume 10 Issue 20

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(20), 2014 [12612-12619]

Research and implementation of user rights management algorithms based on RBAC model for experimental teaching management system

Xiaolin Li*, Yunyun Wei, Xiuzhu Xu, Tao Lu
Hubei Province Key Laboratory of Intelligent Robot, Wuhan Institute of Technology, Hubei, (CHINA)
E-mail: lxl989898@163.com

ABSTRACT

The current experimental teaching management system has a large number of users than before. This problem causes the higher security requirements, complex management and lower efficiency of the teaching management system. Through the comparative analysis of the existing several kinds of access control mechanism and management algorithm, the role-based access has more advantages, we choose role-based access control model (RBAC) user permission management algorithm to build the bridge of users and permissions to increase flexibility and security by introducing user role. By Contrasting with these models response time, the simulation experiment proved the RBAC model is appropriate in the experimental teaching management system.

KEYWORDS

Access control; Role-based access control; Minimum permissions.

INTRODUCTION

With the development and popularization of the computer and network technology, using information technology to promote the modernization of education is become an inevitable trend of social development, the digital campus is expanded from a small number of key universities to most of nationwide colleges and universities gradually during the development. We can create multiple information management systems in a networked environment when we construct the digital campus, the experimental teaching management system attract the attention of various colleges and universities as an important part of digital campus construction. At the same time, with the rapid development of digital campus, the expansion of the scale, a growing number of users, digital campus network security mechanism problems followed. Therefore, a unified system of a higher security authentication and access control mechanisms generating becomes a focal point of the digital campus construction.

The experimental teaching management system as an integral part of the digital campus construction building is facing some of the following areas difficulties:

User features

The great number of users and the limited number of administrators. Different applications correspond to different users and access control module, besides, we need a dedicated administrator to operate during the authorization management process. The repeat of the user information and the frequency of the business rules changes increase the user's job duties, so that they increase the workload of administrators and reduce the efficiency to a certain extent.

Data and security features

When we face numerous teaching data of management needs, how to deal with the problem of sharing data among the different levels, how to assign permissions effectively, how to make a unified capability of identity authentication and authorization management. These problems make improving security issues become an urgent problem.

Discretionary access control (DAC) is the first proposed access control system. It restricts the access to objects based on the body identify. It can control the main direct access to the object and the main can decide access privileges. This presentation is intuitive and easy to understand. However, the customer relationship caused by the relative dispersion of resource management is not reflected in the system, so that it is difficult to manage and the information flow can’t be protected effectively. It leads the disclosure of information easily.

For the lack of DAC, many researchers proposed some method to improve it. Such as in the 1976 Harrison MA, Ruzzo WL and Ullman JD proposed semi-autonomous HRU access control model that expanded the DAC model. It is a combination of the object master self-management object access and security administrators to limit access free diffusion[1]. In the 1992, in order to express the main access, Sandhu developed HRU model into a TAM (Typed Access Matrix) Model[2].

The low security still exists, although researchers have improved DAC. In order to improve the safety issues exist in DAC that the Mandatory Access Control (MAC) is proposed. The MAC originated in the U.S. government and military security regime. It is a kind of grid-based access control. This control model improves the existence problem of DAC security.

However, the MAC has inadequacies on the two sides: application field relatively narrow and integrity relative lack. Researchers proposed some method to improve the lack of MAC. Such as Brewer Nash developed Chinese Wall is a commercial areas access control model[3]. In order to strengthen his integrity control, in the 1973 the BLP (Bell-LaPadula) model was made a lot of improvement on classical model of muti-level security field by Bell and La Padula[4]. In the 1976 Ken Biba proposed Biba. The Biba protects the integrity of the data by two rules of reading property and writing property, besides, it protects the data confidentiality comparing with BLP model[5].

With the changing of information society and the development of security requirements, the deficiencies of DAC and MAC make them been unable to meet the needs of people fully.

In the 1992 Ferraiolo and Kuhn gives the basic definition and terminology of RBAC model from the National Institute of Standards and Technology[6], but it does not get people's attention for a long period of time. In the 1990s, RBAC has aroused great concern for the development of security requirements and R.S.Sandhu’s advocating and promoting[7].

After 1994 Ferraiolo raised the earlier formal definition of RBAC model. Sandhu defined RBAC96 model as a more complete framework[8].

In 1997, they further proposed a distributed management model[9] --RBAC97. It realizes the distributed management based on RBAC model. The majority of role-based access control studies are based on these two models as a starting point.

In 2004, The National Institute of Standards and Technology (NIST) standard RBAC model consists of the four component model: Core RBAC, Hierarchal RBAC, two separate parts of Responsibility of RBAC constraints (Con-straint RBAC), Static segregation of duties (SSD) and dynamic separation of powers (DSD) model[10].

After 2010, the RBAC model is widely used in the world's top 500 enterprises to promote the RBAC model development in various fields. Nowadays, the RBAC model focus on the design of optimization and specific aspects implementation of this model, such as, in the literature[11] Role-based access control model in the design and implementation of information systems in the web, combined with web access features corresponding improvement and expansion on the RBAC model and integration advantages of various models to design and implement for each specific module. There are similar studies with literature[12]. In the literature[13] Based on RBAC model the design and implementation of the vocational colleges management system. After using RBAC model designs specific module, in order to maximize the stability and security probably to perform testing of functions. But it is few relatively about compared to the study of experiment of the superiority among RBAC, DAC and MAC models.

During Teaching Management System construction in Wu Han Institute of Technology, there are large number of concurrent users, information and fewer administrator problems. How to achieve distribution effectively and improve work efficiency under ensure security become a key issue of the construction process concerns. Through the analysis of the development process, specific characteristics and experimental data of the various models. It is proved that the RBAC model are more flexible, faster response time in the case of multi-user concurrent, so the RBAC model is more appropriate in the experimental teaching management system.

ROLE-BASED ACCESS CONTROL MODEL

RBAC model treats the process of permissions authorization as a problem among Who, What and How. In the RBAC model, access triples is composed of Who, What and How, it can also be seen as " a operation of How conducted by Who on What". A formal definition for RBAC model is following:

Who: Principal or the owner of permission, for example User, Group, Role.

What: Objects or resources, such as Class etc.

How: Specific permission, as Privilege.

The difference of RBAC mode between DAC and MAC mainly is its core and the main idea which introduce the concept of role. Role acts as a bridge connection between the user and permissions, the previous user - permission levels structure, transforming to the user - role - authority tertiary structure. The shift can control the user access to resources better. RBAC model shown in Figure 1:

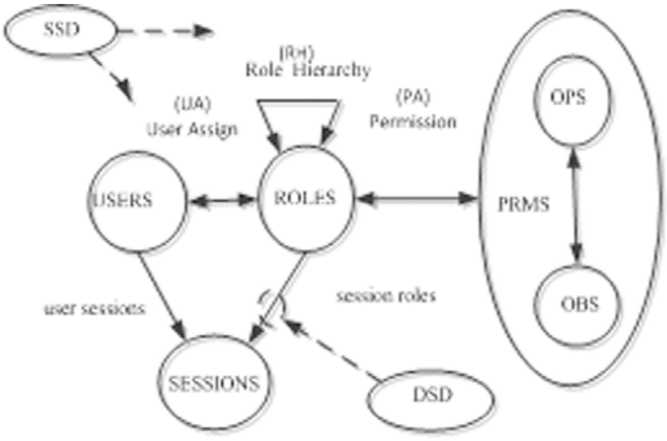

Figure 1 : RBAC model

After induction, RBAC entities can be described from the following aspects:

A. Resources: System resources, mainly contains various business objects, for example, we can download experimental data and other various objects can provide user access.
B. Action: Resource access methods may exist, such as add, delete, modify, etc.
C. Permissions: Licensing about role to perform operations on the object, it is a combination of resources and operations.
D. Role: a collection of system-specific permissions, such as system administrator, general manager or college.
E. User: the main system activity participation, such as people, systems, etc.

The relationship between the various entities: a user has multiple roles and a role has multiple permissions. A privilege refers to a resource of some operations. In practical applications, RBAC create the appropriate role of the specific jobs and their respective roles granted based on the user's terms. When the users are granted permissions, they can obtain the permission to access to resources and then operate the resources.

AUTHORIZATION CONTROL MODULE ANALYSIS IN THE EXPERIMENTAL TEACHING MANAGEMENT SYSTEM

In the experimental teaching management system, we can use the core idea of RBAC by assigning the appropriate role to the user and allow the user to contact access permissions. According to the user in the teaching process to complete different teaching, learning and management tasks and responsibilities and powers in actual life, the user is divided into four types: system administrators, teachers, students, roles. It is convenient to transform flexibly between the users and improve the efficiency.

Permissions need to focus on key issues in the management module, system character and the roles that the user belongs to, the user can access data object access authentication and how to do it.

Experimental teaching management system is an information integrated management system, it is geared to the needs of 1336 teachers and 25879 students, it has many functions, such as online examination, teaching resources management, excellent teaching courseware resource downloading and interaction between the teachers and students for all teachers and students to provide an interactive information network platform. In order to realize the unified classification management of multiple users, user account management, it will be verified by our personnel and real-name registered personnel unified data import, system administrators, on-line control will be authority allocated and managed.

In terms of role assignment, according to the different specific organization of each department personnel responsibilities and jobs, the role of this system is divided into five types: system administrators, responsible professor, teacher, student, department of administrators. According to different departments caused by different identity of teacher user, at the same time, system administrator assign roles, they create and modify the role of our department,

After users determining their role, they can associate and use the permission to have a access to certain data objects; Responsible professor has the rights that the general teachers also have, in addition,he has the rights of add, modifying and maintaining data resources, participating in the experiment project item management and counting the rules; For students, they are only allowed to browse their information (for example: personal information, scores query, experiment schedule, etc.); Department manager only need to browse all kinds of resources (such as: browse the student performance statistics, pass rate, class size, etc.) but can't operate them.

Roles are used as the user permissions mediation, roles and permissions form two many-many relationships, become the key to the current system access control.

The design of access control is the core of database design. The database management system records the users and roles information, stores all system defined by the user, role, user roles, users belong to subordinate departments, information such as the role of permissions. According to the requirements analysis phase of the design, in the Oracle database we design Users table, Role table, User_Role table.

The Users table's main function is to check the legitimacy of the logged in user, user get proper permissions accordingly. The users table of main structure as shown in TABLE 1:

TABLE 1 : Users table

Field name	Data type	Field description
An	Number	Serial number
Actn	Varchar2(16)	User job number or student number
Pwd	Varchar2(16)	User password
Actid	Varchar2(32)	User id number
Actname	Varchar2(10)	Username
Act_department	Varchar2(10)	User department

Important issues in the RBAC model of access control is the character set. Character set must first understand it and the relationship of each element. A role in the access control policy is a one-to-many relationship with permissions. Any known roles, must correspond to at least one access policy. At the same time an access policy belongs to multiple roles. Role table shows the Role of system information, table structure as shown in TABLE 2:

TABLE 2 : Role table

Filename	Data type	Field description
Rolid	Char(2)	Role number
Groupnam	Varchar2(128)	Role name
Usegroup	Varchar2(128)	Role description

The character set in concrete embodiment of the system as shown in TABLE 3:

TABLE 3 : Character Set

Rolid	Groupnam	Usegroup
00	System administrator	Administrator
01	Teacher	Teacher
02	Student	Student
03	Exteacher	Exteacher
04	Depadministrator	Depadministrator

User_Role table, Specifies the user assigned the role of information. TABLE 4 shows the relationship between them.

TABLE 4 : User_Rol

Filed name	Data type	Field description
An	Number	Serial number
Actn	Varchar2(16)	User job number or student number
Rolid	Varchar2(32)	User role

Rights management module of the base table consists of the above table. When the user starts system and landing, it compares the user with the database table at first to confirm the User identity legitimacy, and then the procedure gets the ROLID of the users from User_Role table. Put the User personal information and number to the session variable. Finally user role table determines the authority function. The user gets into work home page by his role, which corresponds to show users that they shall have the right to operate the system function interface, and then realize the function of the system of automatic configuration.

From the module design, we construct the responding rights management module by collecting different role characteristics and operational data to ensure each role to complete his job as little as possible during an operation, namely "least privilege". On the one hand make sure every role in the under privilege to complete the required task or operation; On the other hand give the role the privilege of "essential" limit for each subject can operate. Authorized reasonable can reduce errors, network data tampering and cause unnecessary losses. Users, roles, and thus be considered the specific data collection, collection operations, and so the relationship between objects, least privilege model is set up. The establishment of the minimum permissions model specific process is as follows:

The establishment and the corresponding collection

In the system of permission sets: $PRMS = \{p_1, p_2, \cdots, p_r\} \subseteq OPS \times OBS$.

Establish minimum privilege set

a. Find the smallest behavior of role to complete its task performance action set $OPS(r_i)_{\min}$ and minimum data object sets $OBS(r_i)_{\min}$.

b. Multiply the Cartesian product of two, namely： $OPS(r_i)_{\min} \times OBS(r_i)_{\min}$.

c. Overlap the Cartesian product and system permission $PRMS$, the result is the role of the minimum privilege set, namely $PRMS \bigcap OPS(r_i)_{\min} \times OBS(r_i)_{\min}$.

According to the specific process of the above, we can get the experimental teaching management system, the rights management module algorithm1 is as follows:

Algorithm1 : The rights management module

Input: users use the user work number or student id to log in.

Output: according to user role relational tables, showing its role should login interface.

Process:

Establish the corresponding collection, find the minimum privilege set role, establish the minimum user permissions.

To find the minimum behavior character ri to complete its task performance action set $OPS(r_i)_{\min}$ and minimum data object set $OBS(r_i)_{\min}$.

Multiply the Cartesian product $OPS(r_i)_{\min} \times OBS(r_i)_{\min}$.

$PRMS \bigcap OPS(r_i)_{\min} \times OBS(r_i)_{\min}$ is the requested minimum privilege set, which determines the user minimum permissions.

The establishment of least privilege makes users completes the task of corresponding to its identity effectively and will not be granted with too much authority. When a character has an access to a resource, if the operations are not within the authorized operation of main current role, it will not be able to have the access. When the system is granted with the minimum permissions, role inheritance, authority separation after basic safety principles, the advantages of RBAC can be exerted fully.

OVERALL IMPLEMENTATION OF EXPERIMENTAL TEACHING MANAGEMENT SYSTEM ACCESS CONTROL

Access control of experiment teaching management system mainly includes authentication and authorization management. Identity authentication uses filters Filter(Filter provides an object-oriented modular mechanism for the common tasks package in the components, which is used to take the public task into pluggable components, these components are declared and handled by a configuration file). Assignment of access rights consists of user’s role assignments and role’s operational permissions assignments. Thus the access control process can be divided into the following:

A. By configuring the filter to filter invalid user connection requests to avoid unauthorized users log into the system directly by inputting URL directly in IE. Making use of filter to set s page caching limited on necessary pages specified(contain sensitive information)and to avoid the case of clicking the "back" button bypassing the server-side filtering case of reading directly from the page cache data locally under not closing your browser.

B. When user login authentication to find the existence of the current user in the user table of the database or not, if it is present, they find the role permissions based on the Role ID. Returns the user's permissions information in the Session then calls for the rest of the global variables in the system. In the course of the entire program running, the system can obtain the information of user’s permission and determine whether the current role’s working is legal according to user permissions identification code and its role permissions. In addition, user can modify their own password, when the password is lost, system administrator can modify.

C. Reading privileges data from the Session after user authentication permissions program, determine the user operable function modules during terms of reference and the corresponding button on the role of engineering page by the minimum sets of permissions. Such as add, delete, modify, etc.

D. When user login system, if they does not operate anything in a certain period of time, the system will exit automatically. Procedures set session variable survival 10 minutes in that time, if no request is considered, the connection fails. While the session to keep original legitimate user’s access data, user number and other important information will fail. This method prevents unauthorized users to perform operation by entering the URL address bar as legitimate users effectively.

According to the Ministry of Education teaching level job requirements, this system combines with the actual situation of the university's specific to use Asp as a script service environment to combine with the Oracle database, Dreamweaver as a development tool, B / S as the framework, combine with RBAC introduced roles through role inheritance, segregation of duties to improve work efficiency effectively, to realize the experimental teaching management system based on more than 20,000 people in the school.

This paper proposed RBAC-based experimental teaching management system has been successfully applied in Wu Han Institute of Technology Digital Campus Information System. It is proved that the system is flexible and efficient configuration and control access for users in experiment teaching management system. This section further demonstrates its application results using the practical application data, data of various applications indicators shown in TABLE 5:

TABLE 5 : RBAC application index data table.

Number of users	20030
Number of users	31
Number of application subsystem	18
Number of pages needed for access control	469
Number of operations needed for access control function point	436
Operation requires access control data	29
RBAC relationship table records	38469
Once a user page access time required to verify	0.05s
User page once the time required to verify the operating authority	0.03s
User page once the time required to verify the operating data rights	0.03s

From the TABLE 5, we can see, RBAC is suited to have an access to a large amount of resources, authority flexible configuration, real-time demands of experimental teaching management system.

TABLE 6 : RBAC experimental results data sheet

Number of concurrent users	Response time (ms)	CPU's utilization(%)	Use memory(M)
1000	300	64	1
2000	440	73	3
3000	560	80	3
4000	820	85	6
5000	900	90	6
6000	1000	92	7
7000	1200	100	7
8000	1400	100	9
9000	1600	100	10
10000	1800	100	12

As we can see from TABLE 6, the average response time is also increasing when the number of concurrent users is increasing. The average response time in one second when the number of concurrent users is less than 6000. This time, we can ignore the relative data transmission corresponding to the transmission time from the server to the client in the entire system. With the increasing of the number of concurrent users, the use of server memory usage and CPU varying degrees increase in the extent, when the number of concurrent users is higher than 7000 the CPU usage reaches100%. However,they cannot bring the server loading problems because the response time of RBAC permissions verification of concurrent users are millisecond.

According to the data in TABLE 7, we can see that the difference is not particularly large on response time when the number of concur5rent users below 5000 among DAC, MAC and RBAC model. RABC model is better than DAC and MAC when the number of concurrent users is more than 5000 on response time. From that, we can see that the response time of DAC, MAC and RABC is not much different when the number of concurrent users is in smaller cases. RABC has obvious advantages when a larger number of concurrent users. RBAC model is more appropriate for a large number of concurrent users in Wu Han Institute of Technology Experimental Teaching Management System.

Comparative Performance Analysis:

TABLE 7 : DAC, MAC, RABC Experimental response time data

Number of concurrent users Response time(ms)	DAC	MAC	RABC
1000	370	330	300
2000	530	480	440
3000	630	600	560
4000	900	860	820
5000	1040	980	900
6000	1120	1080	1000
7000	1340	1280	1200
8000	1520	1460	1400
9000	1730	1680	1600
10000	1930	1880	1800

RESULTS AND DISCUSS

Comparing the response time based on the data of system application indicators and results data of RBAC model in this system, we can see that the using of RBAC system is more appropriate in the large number of users and more complex working environment of experimental teaching management.

CONCLUSIONS

In this paper, we combine with RBAC model and the new characteristics of the experimental teaching management system to establish rights management module. And introduce something related to the users, roles of table structure design process in the database, the application of whole module and the minimal permissions access of roles under the limit of the user permissions department. The design is coherent of users, roles and permissions in the access control module, reducing maintenance burden effectively and not involve the change of security management module and database table structure. To verify the feasibility of RBAC model is practice in the digital campus construction from theory.

But the shortcoming and access control of this article is only considering the user's identity/character, and not thinking about other factors. What we have to do in the future is how to dynamically control user distribution and permissions distribution according to the time, location, and other information.

ACKNOWLEDGEMENT

This research was supported by the National High-Tech Research and Development Program("863"Program,No:2013AA12A202), Surveying and mapping geographic information public industry scientific research project(201412014), the Natural Science Foundation of Hubei Province of China (2012FFA099, 2012FFA134,2013CF125), the scientific research foundation of Wuhan institute of technology, projects of the Educational Department of Hubei Province of China (B2013219,Q20131507,D20141505),Wuhan Planning Project of Science and Technology(2013010602010217), Project from Wuhan Information Industry bureau.

REFERENCES

[1] A.Harrison Michael, L.Ruzzo Walter, D.Ullman Jeffrey; "Protection in Operating Systems". Communications of the ACM **19(8)**, 461–471 **(August 1976)**.

[2] R.S.Sandhu, G.S.Suri; "Implementation Considerations for the Typed Access Matrix Model in a Distributed Environment." George Mason University, Technical Report, **(Feb. 1992)**.

[3] F.C.David Brewer, J.Michael Nash; "The Chinese Wall Security Policy," 206, in Proceedings of the IEEE Symposium on Security and Privacy, 1989, Oakland, CA: IEEE Press, 206-214 **(May 1989)**.

[4] Bell David Elliott, La Padula, J.Leonard; Secure Computer System: Unified Exposition and Multics Interpretation **(1976)**.

[5] K.J.Biba; "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, **(April 1977)**.

[6] D.F.Ferraiolo, D.R.Kuhn; 15th National Computer Security Conference. pp. 554–563 **(October 1992)**.

[7] John Riehards; Flexible Server Arehiteture for the Database Tier.University of Bristol Application Infrastructure, **(2005)**.

[8] Ravi Sandhu; Rationale for the RBAC96 Family of Access Control Models, ACM Workshop on Role-Based Access Control **(1997)**.

[9] Jingsheng Zhao, Wei Zhang, Peng Zhang; Research and Application of an Extended Role-Based Access Control. 2011 International Conference on Computer Science and Network Technology (ICCSNT), 2654-2656 **(2011)**.

[10] "Property Verification for Generic Access Control Models", IEEE/IFIP International Symposium on Trust, Security, and Privacy for Pervasive Applications, Shanghai, China, 17-20, **(Dec.2008)**.

[11] Zhang Xiaoyong; Access control model role in the design and implementation of web-based information systems. Chinese Outstanding Master Thesis. **(2011)**.

[12] Qiao Yanqing; Design and implementation of rights management subsystem based on RBAC model. Chinese Outstanding Master Thesis. **(2013)**.

[13] Shi Yang; Design and Implementation of vocational college's management system based on RBAC model. Chinese Outstanding Master Thesis. **(2012)**.