A New Type of WEB-based Access Control Method

Pang Xiyu[1,*] and Huang Guolin[2]

[1]School of Information Engineering, Shandong Jiaotong University, Shandong, Jinan, 250357, P.R. China; [2]Department of Intelligent Traffic Engineering, Yigou Software Technology Co., Ltd. Shandong, Jinan, 25000, P.R. China

Abstract: This paper has proposed a new type of WEB-based access control method which adopted the "Role-function model" user access control idea. By dividing business functions of the page in the bottom menu on the basis of the Web page organizational structure which is required by system business requirements and the user access control requirements, and using the business function as the basic unit of permission configuration, the user's access to the page, the html elements contained in the page, their operation and other Web system resources are controlled through configuring the relationship among user, role, page, menu and the functions. The practical application showed that the access control model can effectively control user's access to the Web system; in the meantime, it has simplified the user's operation and possesses strong versatility, thereby efficiently reducing the workload of Web system development.

Keywords: Business function, Role-function model, User access control, RBAC model, Role-function model, Validation method.

1. INTRODUCTION

Access control is one of the important measures for ensuing the confidentiality, integrity and availability of the Computer Information System. It aims at ensuring the controlled and legal use of system resources, and makes sure that the user can only access the system resources according to his own permission and no unauthorized access.

Neither the traditional mandatory access control nor the discretionary access control can satisfy the demand of increasingly complex management system for access control due to the shortcomings of their own. RBAC is exactly generated under the driven force of this kind of application demand. RBAC performs permission management from the organizational view angle. It can flexibly express the security policies of business organizations, which is the most widely accepted permission model at present [1-4]. The main idea of RBAC is to bond the authorization and the role, it can assign role to the user and enable the user to access the resources indirectly through the role. This method has realized the logical disjunction of the user and the access permission through introducing the role intermediary, bringing much convenience to the permission management [5]. Among them, RBAC 96 model is a representative one. Fig. (**1**) shows the basic model RBAC 0 in the model.

There are five elements contained in the RBAC: users (USERS), roles (ROLES), objectives (OBS), operations (OPS) and permissions (PRMS), the permission is given to the role instead of the user, when a user possesses some role, then it possesses the permission contained in the role. The session means the relationship between the user and the role; the user must activate the role through creating a session every time and obtaining the corresponding access permission. RBAC model is an access control method that has been put forward against the traditional information system, but the Web system has different characteristics from the traditional information system; with the extensive use of the Web application mode, it is necessary to make proper changes of the RBAC model according to the characteristics of Web system, to make it better meet the requirements of the Web system.

Based on the study of RBAC model and characteristics of Web application system, this paper has proposed a kind of "Role-function model" based user access control method to realize the user authorization management with strong versatility, convenience for user, without additional Web system development workload and with controllable granularity through considering the relationship among the user, role, function, menu and page.

2. THE DEFICIENCY OF RBAC USED IN THE WEB APPLICATION SYSTEM

The permission in the RBAC model is to allow the operation conducted on one or more objects, but the object and operation in the RBAC model are abstract concepts, thus resulting in the diversity of permission definitions. Therefore, while defining the object, operation and permission in the Web system should be based on the characteristics of the Web application system itself, and sufficiently study the constitution form of the Web application system page, menu and functions. Only then the ideal Web application system permission management function can be designed. The permission management in the Web application system mainly reflects that the pages that can be accessed through the browser by different users may be different, as for the same page, the data observed and the operation conducted may also be different. If the user wants to complete some task, it can be only realized through accessing the page.

*Address correspondence to this author at the Shandong Jiaotong University, Shandong, 250357, P.R. China; Tel: 15069092175;
E-mail: wangcheng_1001@163.com

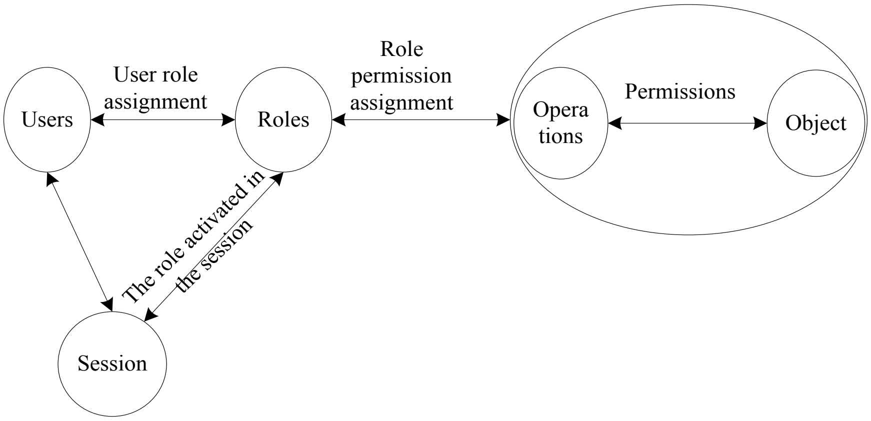

Fig. (1): Model RBAC0.

Firstly, with regard to a Web application system, according to the user's access permission, split the business functions realized by the page and regenerate multiple pages. Corresponding operation can be conducted by the user's access permission to the function that can be completed by some regenerated page, and as the only form of expression of Web application object--page object, its operation is limited to operation, for example, realizing the user permission management through controlling the visibility of the page to user put forward by "Web user access control method based on role-page model". However, the granularity of permission control depends on the division of the business functions with the page as the basic unit, the granularity of permission control will be too large if the function division based on the page is too rough, and if the function division based on the page is too specific, then the problem of large page amount will occur. "Access control design and application facing Web application system" organizes the page through the module. The module is the basic unit of permission configuration; according to the demands of permission configuration, the business functions realized by the modules can be flexibly dispersed into the pages contained in the modules, and the problem of large page amount caused by specific page function division can be better solved [6]; but in the permission control method put forward by the "Access control design and application facing Web application system", one page only belongs to one permission configuration module, implying that one page can only realize one business function or part of it and the existence of redundant page still cannot be avoided thoroughly, for example: through the page, the fields in some table in the database seen by a different user may be different, but the operations may be the same. According to the permission control method of "Access control design and application facing Web application system", multiple permission configuration modules shall be configured according to user segmentation, and certain amount of abundant pages undoubtedly will be generated when different users are allowed to see different data.

Secondly, the difference of role and permission on abstract level usually leads to the difficulty in permission configuration. A role refers to a post in work in concept, while permission refers to the operation of data; role and permission are concepts of different level. The existing RBAC study has not given out clear standards and corresponding instructions on whether a role shall conduct operation for some data in work or not, how to configure to access permission in a most appropriate way, to not only satisfy the system demands but also be convenient for non-computer professional users to use. In the permission control method proposed by "RBAC-based universal permission management system in ASP.net", the menu, page, fields and operations have been abstracted as unified system resources, the access control granularity can be refined to page fields, however, in order to distinguish the fields and operations of different pages, it needs to store the fields and operations of every page; along with the increase of page, role and user amount, the user permission calculated amount increases exponentially. On the page in Web application system, the function of enabling people of different identities to see different data fields can be realized through using one page to support multiple permission configuration modules, which is to allow one page to continuously integrate many similar business functions. User type accessing different fields generally is less than the amount of the fields in the page, and all the operations in the system can be independent to reduce the calculation of permission management; since it is to support multiple permission configuration modules through integrating many business functions in one page, the permission in the permission management module is closer to actual business and convenient for permission administrators to use.

3. PERMISSION MANAGEMENT SYSTEM DESIGN BASED ON ROLE-FUNCTION MODEL

Combining the characteristics of the Web application system and the shortcomings of RBAC application in the Web system through deeply analyzing the logical relationship between page and function in the Web application system and the relationship between function and permission configuration module, this paper has put forward the user access control method based on "role-function model". The model diagram is shown in Fig. (**2**).

In this permission management model, the following relationship exists among page, menu and business function.

1. The business function can be realized by one or more pages, each page can realize one or more operations of one business function (such as view, add, modify, and delete etc.), the operations of multiple business functions also can be realized.

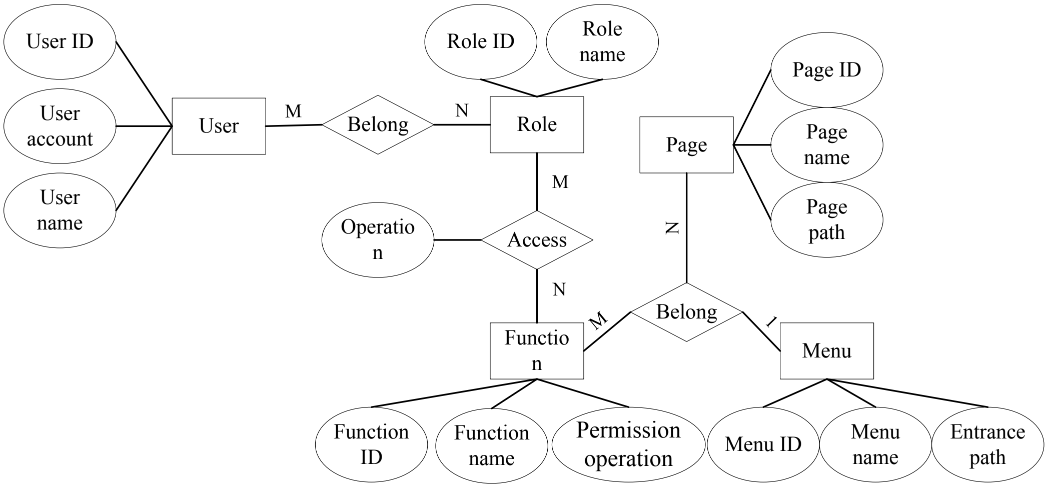

Fig. (2): Permission management model based on role-function model.

2. Each bottom menu is composed of one or more pages, and has one entry address, that is the page address shall be shown when clicking on the menu; each function page only belongs to one bottom menu. The bottom menu and parent menu shall be organized in tree structure.
3. One bottom menu realized one or more business functions through pages, one business function is only realized through the related page in one bottom menu.

For the purpose of access control, the business function configuration shall be conducted for page and menu in the permission management model to indicate that the business functions shall be completed by the pages and menu; and the entry page of the bottom menu should be configured to indicate which bottom menu the function page belongs to. Each user in the system belongs to one or more roles, each role has corresponding access permission for each business function, and the users belong to these roles also have the access permission of the role, especially, for the situation of one user belonging to multiple roles, the permission of the user is the union of the permission possessed by each role [7]. The access management system based on "role-function model" will conduct user access control from the following aspects.

1. User identity authentication: When the user logs in the Web system with account and password, the system will verify the user's account and password, and check whether the user is valid user or not. If it is an illegal user, the access to the system is denied; valid user is allowed to access the system, and read the access permission information and store it in the system cache (Catch *etc*) [8, 9].
2. Dynamic system menu: Since different users have different roles, therefore they have different access authorities of system business functions. After the user entering the Web system, it needs to identify the business functions that the user can access according to the user's function permission access information. So long as the user has the permission to access any corresponding business function of the bottom menu, the user has the permission to access the bottom menu; otherwise the user does not have the permission to access the menu. If the user has the permission to access the bottom menu, he also has the permission to access the corresponding parent menu [10-12]; otherwise the user does not have the permission to access the parent menu. According to the tree structure relationship between the user's access permission of the bottom menu and the menu permission, thereby dynamically create the system menu can be accessed by the user. When the user can access a page and conduct the page access, highlight the corresponding bottom menu and parent menu of the present page according to the menu configuration in the page.
3. Page operation permission verification: The User_A accesses a page, the system will judge whether the user has the permission to access the page according to the business functions realized by the page and the access permission of USER_A for corresponding business functions. If USER_A doesn't have the permission to access the page, then it will be kept out; if USER_A has the permission to access the page, then it needs to further judge the operations of the corresponding business functions in the page that can be conducted by the user according to the access permission for business functions of USER_A; for the operations that the user has no permission to conduct, corresponding page elements shall be hidden or disabled. Among which, the logic for determining whether the user could enter the page can be encapsulated in the base class of the page, uniformly judge whether the user has the permission to enter the page through calling back the business function configuration of the current function page; for the functions in the page the user can use and the corresponding operations, a set of public user control with built-in permission judgment can be prepared to simplify the implementation.

4. KEY IMPLEMENTATION OF ROLE-FUNCTION MODEL

The permission management model based on "role-function model" proposed in this paper has been implemented by adopting the development platform based on asp.net 3.5 and Microsoft SQL Server 2500 and using the base class page, master page and custom control in the

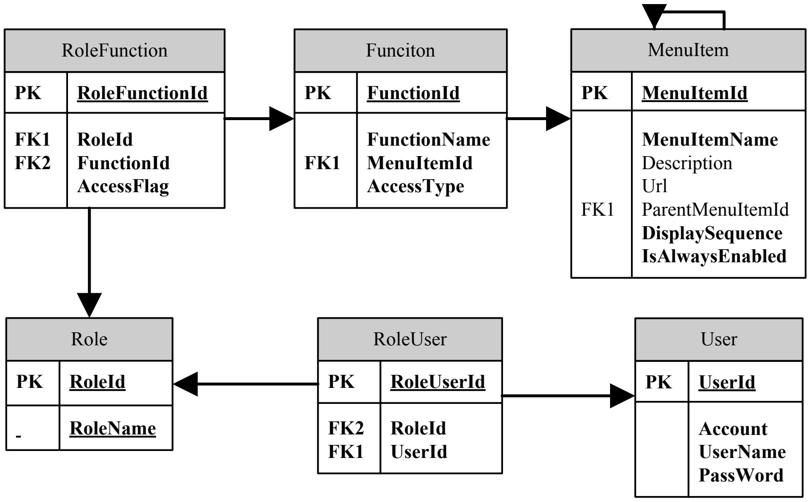

Fig. (3): Database table related to permission management.

asp.net 3.5, and proved the model can effectively control the user’ s access of the Web system.

4.1. Tables Related to Role Management

Database table related to permission management (the underlined fields are major keys; the bold fields cannot be left blank):

1. The User, Role, and Role User tables are used to define the user entity and its attribute, role entity and the assignment of its attribute and role entity to the role.
2. Menu Item table is used to define the menu with tree structure. In the Menu Item table, Url fields refer to the URL of the entry page of the menu (the minimum set of business functions), when the menu of the records is not the bottom menu, the value of the Url fields is NULL; ParentMenuItemId field is self-referential (Menu ItemId) fields, which refers to the parent menu of corresponding menu of the records; if the corresponding menu of the records is top menu, then the value of the Parent MenuItemId is NULL; Display Sequence fields refer to the display order of the submenus that have the same parent menu; Is Always Enabled field refers to whether the corresponding page of the menu needs permission validation or not; if the value of Is Always Enabled is False, it means the entry page of the menu is visible to all users and no permission validation is needed; otherwise, the menu entry page needs permission validation Fig. (**3**).
3. Function table is used to define the business functions realized by the menu; Access Type field refers to the business operations (such as add, delete and review) possessed by the business functions. Role Function table refers to the assignment from role to the permission; the Access Flag field in the table refers to the role’ s access permission for the business functions. The two kinds of permissions in the Function table and Role Function table use the unified name, coding and reading method in the system to simplify the management.

The permission implementation adopts the method based on integer binary digit, each integer means one operation, 0 means the operation is not possessed, and 1 means the operation is possessed. Operation for the access permission value and operation mask of some role for a function are conducted, corresponding permission of the mask is possessed if the result equals to the mask, and otherwise, there is no permission.

4.2. Permission Validation Method

The system conducts user access control from three aspects of user identity validation, dynamic system menu generation and page operation permission validation. Check whether the user is valid or not, read the user’s function permission set when the user is logging in, and obtain the bottom menu the user can access according to the function permission, and then create the dynamic menu the user can access through the tree-type organizational structure of the menu. The page operation permission validation occurred while accessing a page and the page data and operation, which are the important and difficult points of permission management. Since permission validation is needed before accessing each page or conducting each operation, we will adopt the On In it method in the Base Page base class to validate the user’s access permission of the page. The On in it method of one page will be started and executed first [10], so putting the permission validation in the On In it method can ensure that the permission validation will be carried out before entering each page, and in the meantime, the workload of writing codes can be effectively reduced.

Specific permission validation methods are as follows:

(1) Fetch the business function list F realized by the bottom menu and the business operation Operation-f realized by each business function f from the Function table.

(2) From the role (may belong to multiple roles) list that current user belongs to, fetch the access permission value of each role that user belongs to for the business function f from the Role Function table, add the access permission values of these roles for f and the access permission Permission-f of user for the business function f can be obtained.

(3) Conduct logical AND operation for Operation-f and Permission-f, if the result is not 0, it means the user has

the permission to access the business function f; otherwise it means the user has no permission to access the business function f.

(4) If the user can access the business function f, then it can access the bottom menu and its parent menu that realizes the business function; if the user cannot access any business function realized by some menu, then it cannot access the menu.

(5) When the user needs to enter a page p, if the page is always visible for the user, then cancel the permission validation of the user in the On In it method on page p. Otherwise, the Function Names realized through page p return to the function list Fp realized by page p.

(6) For each function fp in the Fp, conduct logic and operation for the business operation Operation-fp obtained from (1) and the current user’ s access permission value Permission-fp for fp from (2). If the logic operation of one business function fp is not 0, it means the user can access the page p; if the logical operation results of all functions fp in the Fp are 0, it means the user cannot access the page.

(7) If the user has the permission to enter the page, then it needs to further verify that the functions and operations in the page can be conducted by the user to control the visibility of each element in the page. Through decoding the function fp access permission value Permission-fp, the specific operations possessed by Permission-fp can be judged.

CONCLUSION

At present, RBAC is a more popular safety control technique. The paper proposed a new type access control authority management, which is on the basis of the full analysis of the relationship between pages, menu and function, and the new authority management takes the function as the most basic unit of permissions configuration management. It can not only avoid the repetitive code due to the introduction of authority management module of Web system, but also reduces the complexity of the authorization management. Therefore, the new authority management reduces the requirement of system administrators. Through the function associated with the menu, the new authority management can realize coarse grained access control of privilege management. Through the function associated with page, it can achieve fine-grained access control. Finally, it shows that the proposed authority management is reliable and convenient, has strong versatility, high portability, and can improve the efficiency of system development through the practical application in the project.

The limitation of the new authority management is that it only realizes the basic model of RBACO. If you need more complex, more functional authority management, you need to do further expansion of the permission management model.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

The research work was supported by National Natural Science Foundation of Shandong Provincial under Grant No. ZR2014FL004 and National Natural Science Foundation of Shan Dong Jiao Tong University Grant No. (Z201215, Z201307) and National Natural Science Foundation of JiNan City Grant No. (201221140, 201221141) and Shandong Province Independent Innovation and Major Project Grant No. 2014ZZCX03402 and A Project of Shandong Province Higher Educational Science and Technology Program Grant No. J15LN12.

REFERENCES

[1] L. Liu, W. Ni, and W. Liu, “Web user access control method based on the role-page model,” *Computer Engineering and Applications*, vol. 42, no. 21, pp. 125-126, 2006.

[2] T. Lu, and G. Wen, “The user access control method under B/S structure,” *Computer Engineering and Design*, vol. 31, no. 7, pp. 143-146, 2010.

[3] M. Fan, Yinghong, and X. Wu, “Universal authority management system based on RBAC of ASP.net,” *Computer Engineering*, vol. 36, no. 1, pp. 143-145, 2010.

[4] W. Yang, H. Zhang, and R. Liu, “A new model based on role access control,” *Computer Engineering*, vol. 32, no. 21, pp. 173-175, 2006.

[5] Y. Xia, and M. Xuan, “The study of unified rights management system based on RABC,” *Micro Computer Information*, vol. 22, pp. 111-116, 2006.

[6] F. Kong, Y. Li, and Q. Zhu, “Access control design and application for web application system,” *Computer Engineering and Design*, vol. 29, no. 5, pp. 1076-1079, 2008.

[7] X. Bian, and F. Zhao, “The study of RBAC model based on the REST style,” *Computer Application and Software*, vol. 26, no. 9, pp. 126-163, 2009.

[8] T. Xue, M. Diao, and W. Pan, “The authority control model based on the user group and object abstraction,” *Computer Application*, vol. 29, no. z1, pp. 112-113, 2009.

[9] J. Chen, B. Dong, and X. Liu, “Research on web based on RBAC in the electronic medical record system”, *Computer Engineering and Applications*, vol. 44, no. 26, pp. 223-225, 2008.

[10] T. Xing, and M. Cao, “Research and application based on TP-RBAC authority tree algorithm,” *Computer Engineering and Design*, vol. 31, no. 5, pp. 950-956, 2010.

[11] X. Zhang, H. Wang, and J. Shi, “RBAC model design and implementation based on the tree structure of web information system,” *Computer Applications and Software*, vol. 26, no. 11, p. 157, 2009.

[12] Y. Qu, C. Pu, and C. Yang, “Research on some key technologies in the development of university teacher management system,” *Computer Engineering and Design*, vol. 31, no. 14, pp. 3323-3324, 2010.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014