ATLANTIS PRESS
Advances in Computer Science Research, volume 63
International Conference on Artificial Intelligence and Engineering Applications (AIEA 2016)

The Comparison of two Different Authority Management Methods on the Base of ASP.NET

Yaoqin Zhu
Qingdao huanghai Colleage, Qingdao, 266427, China.

Abstract. Taking the research and development of H-H Distribution System as background, aiming at the safety problem of user's authority, this essay analyses the requirement of system user's authority management under the B/S mode. The author designs the system function and operation procedure with adopting the safety management strategy on the base of role, and realizes the two different management modes of system user's authority including static state and dynamic with adopting the ASP.NET tech., and makes comparison on the application and capability.

Keywords: ASP.NET; Role; Authority Management.

1. Introduction

This paper introduces an apply the ideas of the role-based access control permissions management method in the Asp.net platform. All access control of the system basically is through the software interface to achieve, through the control of the interface to control the access of subject to object.

2. Basic Principles

In general, a privilege is a formal approval of a particular mode of access to a single or multiple target in the system. Permission is usually positive, which has the authority to implement certain actions in the system. The nature of the authority depends on the details of the system implementation and the specific system. The authority is often used as a symbol that is not explained in the general access control model. The authority management needs to divide the authority in order to correspond to its own resources, it will be further divided in order to facilitate the system to protect it inside each abstract objective and easy to give permissions to the role. A role can be considered as a single or a group of users in an organization to implement a set of operations. The role can be viewed as a set of user's set plus a set of operating rights. The task of role management is to define such a collection, and then assign these collections to the appropriate user. In many access control systems, user groups are usually used as a unit of access control. The management information system is bound to describe the organizational form of the units that use this system, as it must be applied to a certain size of the organization. While users work division according to the user's Department posts or work group to determine the role. Abstract out of the user's objective organization and integrated access control model, which can greatly enrich the performance of the model and makes the system consistent with the objective situation to satisfy user's habits.

There are three kinds of organizational forms in the general organizational structure: horizontal organizational form according to functions, longitudinal organizational form according to tasks (or items, products, etc.), and matrix organization form combining the two. Matrix organization is divided into three types, the weak matrix, the equilibrium matrix and the strong matrix. Rows and columns of the matrix represent the function point and role of the system, the intersection of the ranks of the matrix represents the current role whether there is the use of permissions for the current function.

3. Demand Analysis

H-H sales system is a complex enterprise-class applications, its regional division and job functions are very detailed and complex division. Sales system is the regional division on the one hand, from the headquarters of the management down sub-regions, offices, distributors, users belonging to different

regions can only see the region's data and data. For example, the office of the Northeast is not possible to see the East China office setting, but do not see the operation of other offices. While the staff of the two different offices in the North District could not see the operations of other departments. On the other hand users belong to different levels of job division. Different post staff need to view and operate different data and data. For example, the office staff can only input the contract basic data, but cannot see and modify the contract price, discount and other important data. Headquarters of the management staff also divided positions, the staff of each post can only manage the data of this post. In order to achieve the user's rights management, user access control needs to be specific to each page, and some even a button on the page.

4. Overall Design

ASP.NET has three-tier structure-presentation layer, business logic layer and data access layer, so that the page code and logic processing code and access to the database code are separated from each other and transparent.

All the access control and access control of this system are realized through the software interface basically, through the control of the interface to control the main object of the visit. There are two kinds of interface performance requirements in the system: the visibility and accessibility of the software interface elements; the visibility and operability of the software interface data set. The user is divided into roles by headquarters and office, in which the headquarters can see the information of all offices, and offices can only see their own office information. This requires binding the DataGrid and Dropdown List by the user's role when binding different data. And some of the management and maintenance of the page is the headquarters of the management and maintenance personnel to visit. Headquarters also distinguish the various positions of staff and management personnel. As the office distinguishes between managers and staff, headquarters also distinguish between the staff and management staff. Various positions on the page control and data visibility requirements are different, the operation of the button is not nearly the same. Figure 1 is the user login system and enter the page processing flow. The user login to determine the user table in the user name and password match, the success of the user name and user department stored in the Session. Page application is to determine whether the login judge to obtain the value of the Session user name is empty, authentication authority is to determine whether the user list in the list of permissions to comply with the rules of the page to enter the page. If allowed to enter the page in accordance with the role of the page to determine what kind of control and data loaded.

The user logs in the database and records the user name in the table, login time and login machine IP and other basic information at the same time to increase the security of the system. Users enter a page corresponding to the page name is recorded, and user login information together as the system to maintain the basic log information

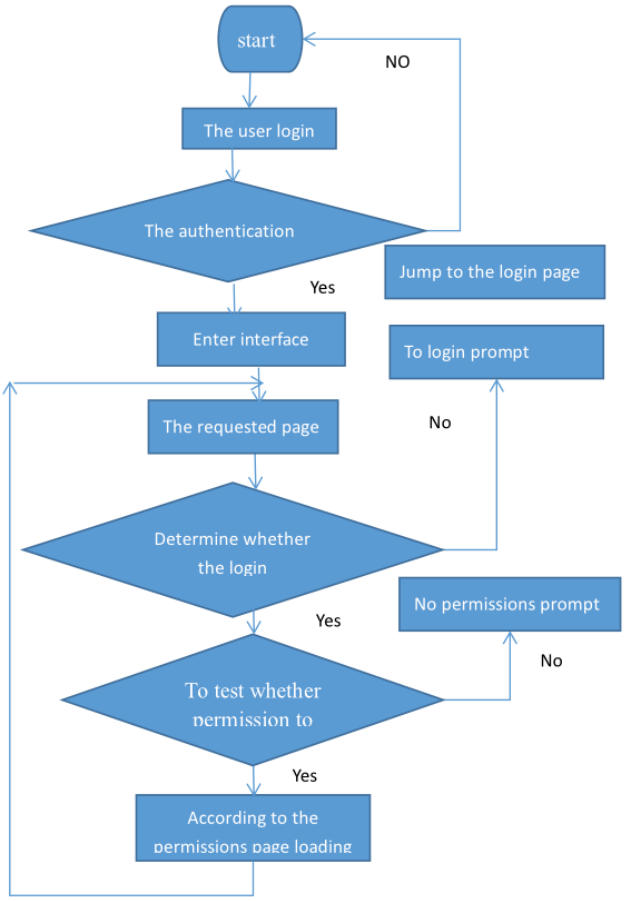

Fig1 Authority judging procedure diagram when entering page

5. Implementation of the role of the static assignment of permissions

5.1 Rights management database design

Static allocation role is the role of the system and the role of each authority has been set, once the design is completed cannot be changed. The realization of this kind of design idea is relatively simple. First design the user table and role permissions table, then set the user number and department number foreign key in the user table, and the numbers are arranged in odd-numbered increments for easy expansion. Specific design as shown in Table 1, Table 2 shows.

5.2 Code implementation

Before accessing each page, remove the permission number and user ID of the user stored in the session when the user logs in. Privileges are defined in the class of each module to define the permissions of the page can access the number. Procedures need to call the authority to determine the class, and the module number and permission number for the parameters of transmission, you can determine whether the user can enter this page. Because some permissions to a page is not specific enough, therefore, in some buttons (such as the delete function button, the audit function button) needs to be carried out to determine the permissions before the operation.

Because the permissions are fixed, the function of the judgment of the function is very simple and easy to write, and the amount of code is not large. It needs to be classified according to the module and then classified according to function, the purpose is to facilitate the call function to find the matching authority number. To compare the number of the passed arguments and the privilege class function after finding the number, if the same is true, it means that you can operate. And on the contrary return false, it will pop up the corresponding prompt box to warn the user. But the downside of this is that the permission number is written to the authority to determine the function, if you want to change is very troublesome.

Table 1 authority characterization table

Field	Type	Length	Primary/ foreign key	Default	Explain	Definition
AID	Smallint	2	P	‘ ’	Access number	
AName	Varchar	50		‘ ’	User name	
AEnable	Bit	1		1	unsigned int flag	0:invalid;1: valid

Table 2 User characterization table

Field	Type	Length	Primary/ foreign key	Default	Explain	Definition
UID	Int	4	P	‘ ’	Userid	Automatic numbering
BID	Smallint	2	F	‘ ’	DeptID	
AID	Smallint	2	F		Access number	
UName	Varchar	50			User name	
UPassword	Varchar	200			Password	

6. Implementation of dynamic privilege management

6.1 Rights management database design

To set the permissions to be flexible, you need to add a table that has special editing privileges. As shown in table 3.All pages and the information that you need to set are in this table, each user's permission set is based on this table.

The name of the page in the table is stored in the page permissions table, the classification field in order to facilitate the sub module management. Sometimes a page for the rights is not enough specific, and some related to the function button to hide, and some related to the hidden data. This type of page will be described in more detail, details are stored in the button name field, form name field, and form attribute field.

Table 3 Page authority information table

Field	Type	Length	Primary/ foreign key	Default	Explain
ID	Int	4			Number
Name	Varchar	50			Name
Page	Varchar	50			Ppage
Sort	Varchar	50			Classify
BtnName	Varchar	50			Utton Name
GridName	Varchar	50			Table name
GDelete	Int	4			Table properties

6.2 Code implementation

The page permissions information table (that is, the information in Table 3) binding to the rights management page in the DataGrid control, as shown in Figure 2.The permissions of each page check box combination of options, according to the bit and the method to calculate the character of this page is the authority of this page information. The number of the records of each page as the number of records, which connects to the permissions string and stores into the user ID field in the user description table.

Fig. 2 authority setting page

7. Conclusion

After the comparison in the system, we can see that the second method of dynamically assigning permissions is more flexible and static than static mode, and it is also very easy to extend and maintain. But its complexity is higher, so the user set the error or the page permissions information table data have fine errors which can lead to the error of the system permissions. There are almost no differences in the running speed of the two methods in the power management system of hundreds of pages. But then modify the permissions based on static power management is very complicated and huge project. So this simple and easy method can be used in small local authority management simple and clear management system. Dynamic privilege management method is applicable to the complex and changeable, and requires flexible adjustment of the medium-sized management system.

References

[1] Damien Foggon, Daniel Maharry ASP.NET 1.1 Introduction to database. yanghao, Beijing qinghua university press. No. 11, p. 31-36.

[2] http://www.ifcem3.org/.

[3] http://www.lsuc.on.ca/with.aspx?id=2147499495#_Networking.

[4] http://www.jstor.org/stable/41166177?seq=1#page_scan_tab_contents.

[5] Meier JD, Mackman A, Dunner M, et a1. Building Secure ASP. NET Applications: Authentication, Authorization, and Secure Communication [M]. Microsoft patterns & practices, 2012, No. 11, p. 31-36.

[6] Marshall D. Net security programming [M]. Yubo, translation. beijingqinghua university press, 2013, No. 3, p. 112-116.

[7] Platt DS. Microsoft. net essence [M]. Huanghuiping, translation. jixiegongyepress, 2014.