The Permission Management Of Access And Control Based On Role In Monitoring Platform

Lihua Jiang[1, a *] , Aixia Zhu[2,b]

[1]School of Computer, Wuhan Polytechnic University, Wuhan Hubei, China

[2]School of Animal Science, Wuhan Polytechnic University, Wuhan Hubei, China

[a]jianglihua@whpu.edu.cn, [b]415593244@qq.com

Keywords: ASP.NET, MVC, C#, RBAC

Abstract: according to the multi-user characteristics in monitoring platform, the article uses the RBAC privilege management model being popular at present, which tell about the design and implementation of permission management, and which explain the system relating, demand analysis, the design and realization of the system. at the same time, it shows the related realization page. The whole design is used by adopting the technology of ASP.NET based on MVC mode, which is developed by C# language. According to the function of each staff, the permission management can allocate the permission so that the whole platform can work safely and stably.

Introduction

Nowadays, freshwater aquaculture is facing many problems which include the pollution of water, the degradation of seeding, extensive cultivation, farmland planting is facing many problems which include the excessive pesticide, improper fertilization and the nutrient loss of soil. In order to relieve the problem of food safety caused by these environmental issues, which develop a monitoring platform of small habitat of farmland and fish ponds, on the base of the NET method of three layer structure[1], this design can realize to use the small ecological environment to monitor permission management of the platform and to solve these problems of the data security and chaos which are caused by many people operating, so that it can improve the security and stability of the whole system.

In order to ensure the safe operation of the whole system, which make the appropriate allocation of the permission for every user according to their levels and scope of work to guarantee the security and stability of the whole system. In present years, comparing the traditional management of permission, the RBAC mode which is base on the control mode of the character accessing and a kind of permission mode used widely simplify the control of permission greatly[2]. In this system, permission management includes the management of character, the institution of organization, the management of user and so on.

The Relative Technology Of System

B/S Mode and ASP.NET Technology. With the development of Internet technology, the browser has become the main platform of displaying the information. The application adopting the browser as the platform to display the data is called B/S application system[3]. Building on the base of the structure of three layers C/S, the structure of B/S has changed or improved the structure of C/S, and its essence is a special case of C/S structure used on the Web. As shown in Figure 1.

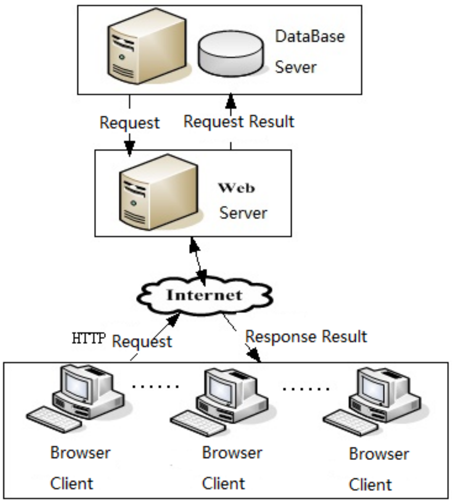


Fig.1. the system structure of three layers B/S

The B/S architecture is generally divided into three layers. And the first layer is client, which is the interface between user and the whole system. Through the browser, user can send a request to the web serve over the network. The second layer is the web server, which receive the request such as the HTTP query and the modification, according to these requests, which gets the related data in the database server and translates the results of the data into the HTTP and other description Language and returns to the browser. The third layer is responsible for managing the database and coordinates these requests from the different web servers through the database server[4].

The ASP.NET is a part of the NET Frame Work and a web script that is developed by the company of Microsoft and embedded in the web page, and that is a server scripting technology executed by the Internet server. When the HTTP requests document, the ASP.NET creates them dynamically on the Web server[5]. The Active Server Pages is a dynamic server page and runs the Internet Information Server which is a Web server developed by Windows.

RBAC Permission Model. The Role-Based Access Control is a new permission control and a best permission control model instead of the traditional access control. In the RBAC, the permission is related to the character. The user can get the permission when they become the appropriate member. Therefore, that can simplify the management of permission greatly. In a organization, the character IS created to accomplish variety of work. According to its responsibilities and qualifications, the user is assigned a role and changes from one role to another easily. According to the new requirements and the systems for merging, the character can get new permission which can be taken back from some character according to the need. The relationship between one character and another can be built to include the wider objective situation.

The main functions of the permission management include the permission control and the adding permission control of system background[6]. To design the database According to the model diagram shown in Figure 2.

In the process of the permission control, administrator can create new user and assign permission. The user need to test identify when log in the system, after the identify pass, administrator can store related information according to the character. When the homepage is been loaded, the permission information gotten by the character can ensure the interface which the user can operate. If the user did not have the right permission, the interface of operation could not be shown.

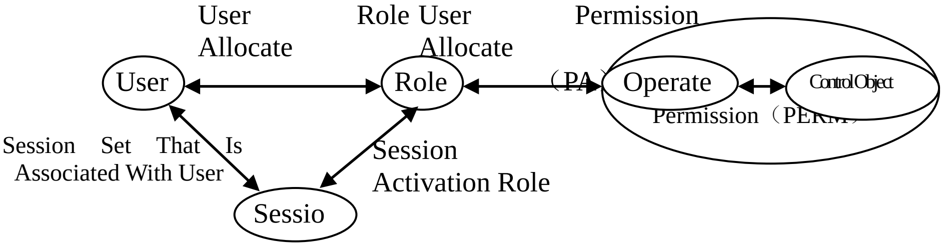


Fig.2. RBAC Model

Needs Demand

In the monitoring platform system of small ecological environment about farmland and fish pond, which join in the permission management to improve the efficiency and security of the system maintenance. The permission management can be divided two parts. One part is the management of basic information, another is the permission management. And the management of basic information includes the information management of the user, department, module and character. The information sustains the whole permission management[7]. When the user visits the page, the permission management can call out the permission that the user own to judge whether the user own the related permission of operation. If the role of the user is empty, which should find the role of department so that which could find out the related the permission operation. The whole system is designed as this way and fully considers all systems which own the function of the permission management.

Needs Statement. A system can be operated by many personals, the permission of system operation should be different according to personnel's different responsibilities, which is the most basic function of the system.

If the administrator is required to assign the system to staff, considering the much more categories of personnel, the distribution of permission would be a time-consuming and inconvenient work. The system will use the group that is the way of the department to distribute the permission. The system will incorporate the personnel who own the same permissions into the same group and then assign the permission to that group. Of course, in order to distribute the diversity of permission, it will retain the right to operate the distribution system[8].

It be convenient to transplant to any system with permission management function as like component that can be reused rather than which should redevelop the permission management for each new management system.

We should assign the right permission for each member like the permission of checking the work themselves department and others. In order to manage the member of each department in whole, we should add the permission group which its setting is the same as each member basically[9]. When the user forgets the password, he can find the administrator to initialize the password, at the same time, user can change the password through the system to protect the security of the account.

The Functional Requirement Of Target System. When the user log in the monitoring platform system of the small ecological environment, he could get in the operational page if he enters the right user name and password, and if the user name and password are wrong, it would return the home page. User can perform the user right management, the news management and the product content management in the operation page. Under the permission management of user, when the user drops down the menu, the system will appear the page of the addition of user, the list of user, the modification of password, the addition of module, the list of module, the addition of character and the list of character. User can modify the information, add role and delete user in the user list. At the same time, user can modify the password. User can modify the permission and delete the role in the list of role.

The Design And Implementation Of System

Overall Design. The overall design of the system is shown in Figure 3. the administrator logs in the system, and then he can enter into the permission management of the user. There are the management of the user, the department, the module and the character under the permission management of user. The management of user mainly preserves the basic information of the user, which includes the operation of adding, deleting and modifying. The distribution of character is the operation of giving permission. The management of user should first retrieve a user under a department when it is given the permission, and then it will modify the character to modify the permission. The department management mainly preserves the basic information of the department, which includes the operation of adding, deleting and modifying. The management of module also preserves the basic information of the module, which includes the operation of adding, deleting and modifying. In addition to preserving the basic information, the management of character also includes the operation of permission to add, modify and delete the permission mainly[10]. The last sub function of user's permission management is modification of password for the security of the passwords.

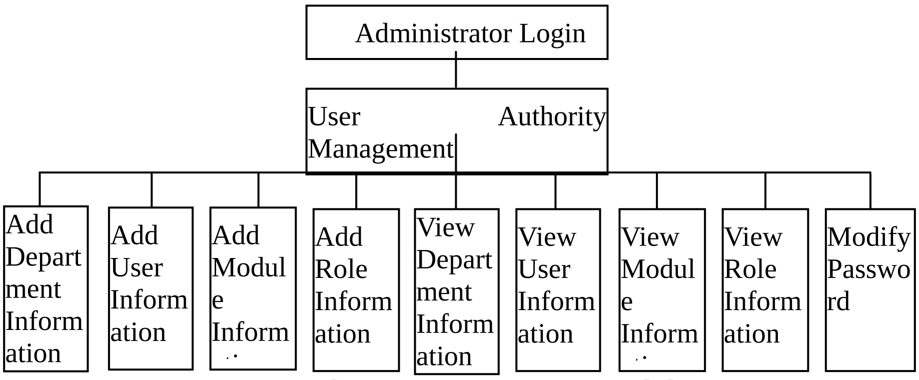


Fig.3. Authority Management Module

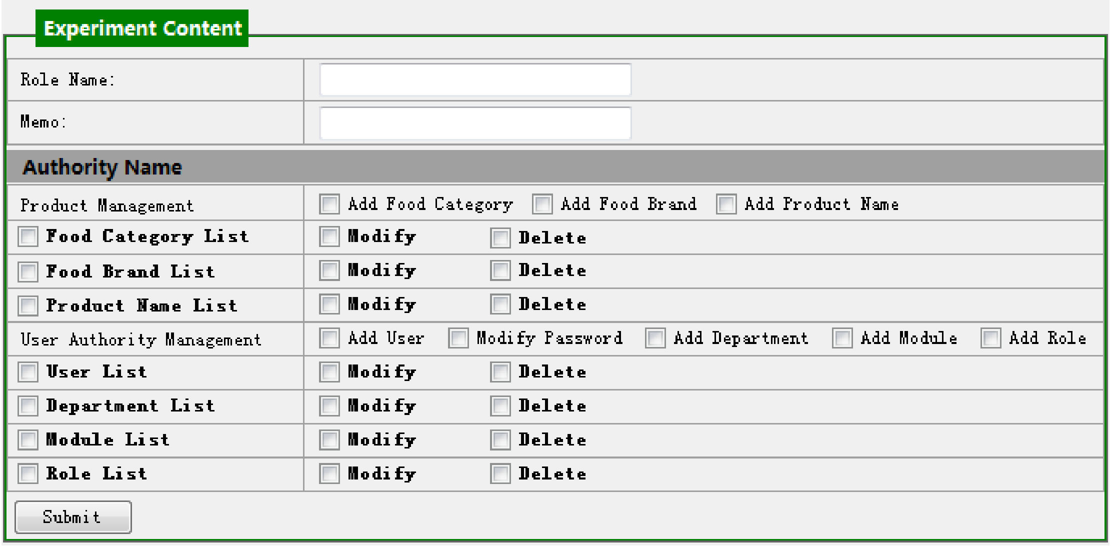
Module Design. The entire process of the user management is shown in Figure 4. When the administrator enters the correct name and password, the controller will receive and compare with the background user, if the match is successful, it would get into the home page of operation. The management of user is categorized to the adding of user and the list of user. If the administrator operates the count of some user, at first, which should look for the department in which the user is, and then which would modify and delete the data of the use. In the process of the user operation, he must have the appropriate permission of operation.

After the administrator logs into the operation of the home page, the department management is divided into the department of add and the list of department. The department of add must give related role that is the permission to the department[11]. Of course, all these operations need these logged users own the right permission.

The module management is divided into the add module and the module list. The administrator looks for, edit and delete the basic information of the department in the module management.

The role management is divided to the role of add and the list of role. When adding a role, which must give the role to the permission, that is, there is no role in no permission. The administrator looks for, edit and delete the basic information of role in the list of role, and it first need check and modify again for the permission modification of role in the list of character. When user gets into the page of modifying the password and enters the old password and the new passwords twice to confirm, the controller will operate the database and replace the current password with the new password.

Category Design. It creates the category for the addition and modification of user. And the category of the CreateEditUser is the category of the business and logic to add and modify the user, which connects the ActiveX of NET to finish the ActiveX of user. In the foreground page receiving the user information, the category will pass the information that the user enters to the database. All these operations take place in the category of the F_User. The Attribute passes the gotten data and the OLEDB modifies the information of database. The user can operate the page before the Session that is recorded after the use logging will judge whether the user owns the permission of operation. Only the users own that permission, they can operate that.



Experiment Content

Role Name:	
Memo:	
Authority Name	
Product Management	☐ Add Food Category ☐ Add Food Brand ☐ Add Product Name
☐ **Food Category List**	☐ **Modify** ☐ **Delete**
☐ **Food Brand List**	☐ **Modify** ☐ **Delete**
☐ **Product Name List**	☐ **Modify** ☐ **Delete**
User Authority Management	☐ Add User ☐ Modify Password ☐ Add Department ☐ Add Module ☐ Add Role
☐ **User List**	☐ **Modify** ☐ **Delete**
☐ **Department List**	☐ **Modify** ☐ **Delete**
☐ **Module List**	☐ **Modify** ☐ **Delete**
☐ **Role List**	☐ **Modify** ☐ **Delete**

Fig.4. Add Role Page

System Implementation. According to the demand analysis of the development permission, the main use IS the personnel of the background management. The administrator can browse several functions of the permission management of user through the navigation menu after the administrator logging, and the several functions are respectively: the addition of user, the list of user, the addition of department, the list of department, the addition of module, the list of module, the addition of role, the list of role and the modification of password. These are some basic settings for the permission management, and which is controlled by the settings for these options[12]. When the administrator logs in the system, which should first judge whether the logged user have the relate role, if there is the right role, the user must be the administrator, if there is not the right roles, which should query the appropriate information of permission according to the department the user is in. Only the user owns the permission, which can operate that, and if not, the system will prompt the user to have no access to operate.

Due to the length limitation, this paper only gives the role permission setting page as shown in Figure 4. The user can select the item of operational function in some item of management to get the right permission of operation. The operation is going on between the addition of role and the permission of role.

Conclusion

We can not avoid to be related with the question of the operation of permission in any complex and multi-user system. The more user the system has, the more complex the problem of permission is. The multi-user system has the similar questions of the permission for the monitoring platform of small ecological environment. The permission management system of the monitoring platform is a set of management system based on the internet, which uses the Browse/Server framework and is the Web server of IIS and the database of ACCESS. The whole design uses the current and popular management model of the RBAC privilege. The privilege is related to the role, and the user gets the permission through becoming the appropriate role. So that can simplify the permission management. The module of design mainly includes the management of the department, the role, the operation, the module and the distribution of role. Some operations in the page address and the page are related to some roles, at last the use is distributed to the appropriate role to realize the function of the permission management in the platform for the department.

Acknowledgments

The paper is supported by the Natural Science Foundation of China (Project No.61502362) and 863Prgoram (Project No.2013AA102302).

References

[1] Designing Distributed Applications, MSDN Library For Visual Studio.net, Microsoft Corporation, 2009

[2] ASP .net Web Forms, MSDN Library For Visual Studio.net, Microsoft Corporation, 2009

[3] McMeekin T.A.Ross T., Predictive microbiology: providing a knowledge-based framework for change management, international Journal of Food Microbiology, 2010. 78:133～151

[4] Soboleva T.K,Pleasants A.B, Predictive microbiology and food safety. International Journal of Food Microbiology,2011.57:183～192

[5] Alex Fedorov，Advanced Delphi Developer’s Guide to ADO, Wordware Publishing,Inc,2008

[6] Dino Esposito.ASP.NET2.0 Technology insider [M]. Beijing: Tsinghua university Publishing,2007

[7] Snyder L. Formal Models of Capability-based Protection Systems[J].IEEE Transactions on Computers,2004,30(3):172-181.

[8] Sandhu R, Coyne E J. Role-based access control models[J]. IEEE Computer,2010,29(2):38-47

[9] Abrams M D, Eggers K W, La Padula L J.A generalized framework for access control: an information description[C]// Proceedings of the 13th National Computer Security Conference. [s.l.]:[s.n.], 2008:135-143

[10] Designing Distributed Applications, MSDN Library For Visual Studio .net, Microsoft Corporation, 2009

[11] Douglas E. Comer, Computer Networks And Internets, Tsinghua university Publishing,2010

[12] Stephen Walther, Active Server Pages 2.0 Unleashed, Beijing Hope Electron Publishing,2011