Forest Chemicals Revew
www.forestchemicalsreview.com
ISSN: 1520-0191
May-June 2021 Page No. 41-51
Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

Authority Management System Design in Forestry Information System Based on Asp.net Three Layer Network Architecture

Chu Shulai[1*], **Zhang Pengwei**[1]
[1]Zhoukou Vocational and Technical College, Zhoukou, Henan, China
*Corresponding Author.

Abstract:

The authority management system of network structure in forestry information system is one of the core security measures of industrial intelligent manufacturing network. In order to deal with a large amount of information, it often takes a lot of time, manpower and material resources to update and maintain the permission information. This paper discusses the three-tier network architecture of professional website authority management system in forestry information system based on asp.net technology. This paper elaborates the functions of user interface layer, business logic layer and data access layer, and their roles in authority management. This paper compares and analyzes the advantages and disadvantages of ASP and ASP. Net technology in professional website design. The experimental data show that the professional website authority management system based on asp.net technology improves the security, scalability and maintainability of the website, and achieves good results.

Keywords: *Forestry Information System, permission information, network architecture, ASP, permission management system, manufacturing network.*

I. INTRODUCTION

In this paper, an extensible user rights management mode in ASP.NET-based information publishing system is proposed. The following will introduce the basic framework of ASP.NET, the basic idea of RBAC, and the complex permission design pattern, and then put forward an easy-to-operate permission control pattern for WEB sites by using web.config and XML technology in. NET. [1-2]

With the increasing popularity of Internet technology and the rapid development of network-based information technology in all walks of life, the issue of network security has become one of the hot topics of current research because of its special importance. The network information system has many users and complex functions, and generally adopts the access control model based on role permission. However, a5p.net technology provides a good security mechanism for the network from three levels: authentication, authorization and simulation. Project management system provides a powerful project management platform for enterprises, which aims to help enterprises successfully complete all the projects. But like other websites, they are facing an important security problem [3]. To ensure the safety of the project management platform is an important prerequisite for the normal operation of the project management system.

II. OVERVIEW OF ASP.NET

ASP.NET adopts a typical three-tier structure, with presentation layer, middle layer and data layer as shown in Figure 1. ASP.NET is a real Object-oriented programming, which realizes the separation of code and program [4].

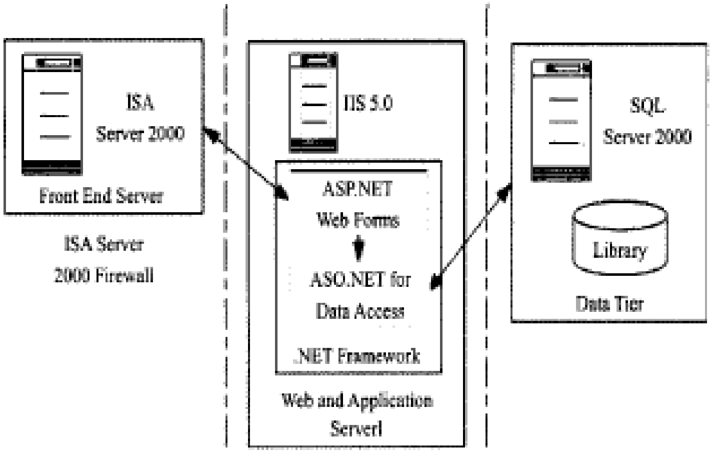


Fig 1: Typical 3-layer structure

2.1 Presentation layer user interface

(1) Net presentation layer is realized by asp.net web forms, which is a program model of upgradable general language runtime (CLR) [5-6].

(2) based on the server-side dynamic page technology, it can dynamically generate general HTML pages independent of the client browser type according to the information requested and submitted by the client.

(3) The WebForms control is responsible for generating the user interface. The separation of

code and content enables asp.net web pages to be dynamically compiled into controlled classes to improve performance.

2.2 Middle layer business logic

(1) Distributed business component is responsible for business logic deployment of enterprise application. It is the key of three / multi tier architecture and the core of enterprise application.

(2) Web service is supported in. Net platform. Web services are network-based and distributed modular components. They perform specific tasks and comply with certain technical specifications, which enable Web services to interoperate with other compatible components.

(3) Web Services think: everything is a service, these services publish an API for other services in the network, and encapsulate the implementation details.

2.3 Data layer database access

(1) Net framework uses ADO. Net to access the database.

(2) Ado.net follows a more general principle, unlike the ADO model, which is database centric. ADO. Net sets all the classes that allow data processing [7].

(3) Asp.net provides three kinds of practical data controls: repeater, datalist and DataGrid controls, which provide flexible methods for data display.

(4) Ado.net regards data as loose, multidimensional and object-oriented, which provides convenience for dealing with multidimensional data.

III. THE BASIC IDEA OF RBAC

The basic idea of RBAC (role-based access control) can be simply shown in Figure 2, that is, the whole access control process is divided into two steps: the access permission is associated with the role, and then the role is associated with the user, thus realizing the logical separation of the user and the access permission. Because RBAC realizes the logical separation of users and access rights, it greatly facilitates the rights management. For example, if a user's position changes, as long as the current role of the user is removed, the role of adding a person to represent a new job or task can be added. The change between roles / permissions is much slower than that between roles J user relationships. And it doesn't need many technologies to delegate users to roles, and administrative personnel can perform them. The task of configuring permissions to roles is complex, requiring certain technology, and can be undertaken by special technicians, but not for them to delegate users, which is exactly the same as the actual situation [8-10].

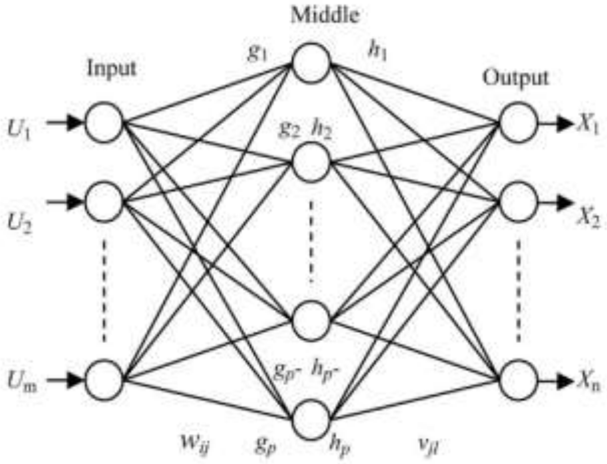


Fig 2: Role access control

A perfect authority design should be fully extensible, that is to say, adding new other functions to the system should not bring great changes to the entire authority management system. To achieve this goal, the first is the reasonable database design, and the second is the application program interface specification.

Generally, permission table and related contents can be described in six tables, as follows:

(1) Role (i.e. user group) table: it includes three fields: ID, role name and description of the role;

(2) User table: it includes three or more fields, ID, user name, description of the user, and other information (such as address, telephone, etc.);

(3) Role user correspondence table: this table records the correspondence between users and roles. A user can belong to multiple roles, and a role group can also have multiple users. It includes three fields: ID, role ID and user ID;

(4) Restricted content list: this table records all data tables, functions, fields and their descriptions that need to be restricted, including three fields: ID, name and description;

Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

(5) Permission list: this table records all the permissions to be controlled, such as register, modify, delete, execute, etc. it also includes three fields: ID, name, and description;

(6) Permission role user correspondence table: in general, the following rules are made for the permissions of roles / users. Roles have the permissions that are explicitly allowed, and others are prohibited. Users inherit all the permissions of their roles. All the permissions within this scope are allowed except those that are explicitly prohibited, and all the permissions outside the scope are prohibited except those that are explicitly allowed.

IV. ANALYSIS OF THE SECURITY REQUIREMENT OF THE SYSTEM

The security threats of project day management system mainly come from the following aspects.

4.1 Threats from DBMS itself

As the project management system is a large transaction processing system, its database system should run stably and safely. Therefore, we should prevent the system from crashing (including OS and DBMS) and restarting, so as to avoid the integrity of the data in the database being damaged due to the loss of data in memory.

4.2 Threats to the whole system from people inside the project management system

Because there are a lot of users using the system, the work done by each user is not the same, that is, the permissions assigned to each user are different, and some users may carry out unauthorized operations with their legal identity.

4.3 The threat of external personnel (such as hackers) or other factors to the whole system should be prevented

This is mainly manifested in the following aspects:

(1) The system is a multi-user system, so it is inevitable for attackers to use the identity of a legitimate user to log in to the system for "fake attack".

(2) In order to obtain the identity and login password of a legitimate user, the attacker may take "home page" deception.

(3) All data processing in the system is realized through the network, how to ensure that the information receiver (sender) can not deny that he has received (sent) a certain information is also a security problem faced by the system.

V. SECURITY TECHNOLOGY DESCRIPTION

5.1 Role based access control (RBAC)

RBAC (role base access control) plays a very important role in the application layer security control of the system. The core idea of RBAC is to associate the access right with the role. By assigning the appropriate role to the user, the user can be associated with the access right. Role is a specific task category that needs to be set according to different tasks in the enterprise. The system sets users' roles according to their responsibilities and responsibilities in the enterprise. Users can switch between roles.

5.2 Security technology of ASP. NET

(1) Authentication (authentication)

Authentication is to identify the user who requests information. The authentication in the ASP.NET identity list is realized by an authentication provider, which contains a code module for authenticating requests from customers. ASP.NET provides ASP.NET and ASP.NET+IIS. It not only supports Microsoft's Passport verification service, but also unilaterally provides sign-in service and user description service; And that purpose is to provide cookies to help establish an authentication mode based on us Forms. Cookies enable users' applications to implement user-defined trustworthiness verification with their own code and logic. ASP.NET provides a variety of methods to authenticate users, each of which is realized by an independent authentication provider, such as Windows, Forms and Passport. Next, these authentication methods will be introduced.

① Windows certification

When requesting ASP.NET, the customer first encountered IIS, Microsoft's WEB server. At this time, IIS will authenticate the user or hand over the work to the ASP.NET application; When IIS handles authentication, it can directly communicate with the operating system to verify the user's credentials.

②Form authentication

In ASP.NET, ASP.NET application (instead of IIS) can choose to authenticate through forms, which gives users greater control over the authentication scheme of the site, and can store the user's credentials in a database or XML file instead of Windows system.

③Passport certification

Passport authentication is a centralized authentication service provided by Microsoft Corporation. Its working principle is very similar to form authentication, except that it does not need to create any custom functions. In both methods, when the client creates authentication cookies and uses Passport authentication, the user will be directed to the Passport login page and let the user fill out the form, which will check the user's certificate through Microsoft Passport service to determine whether the user is legal or not. Then set an authentication cookie like form authentication. Passport authentication service does not create authentication cookie, which is done by the original Web server.

(2) Authorization

Authorization is another important function provided by security system, which aims to determine which resources can be accessed by authenticated users. ASP.NET provides two authorization methods, i.e., authorization method based on ACL resource rights and URL authorization.

(3) Impersonation

Act as a user who enables ASP. NET to execute a page by running a client program. If a user is authorized as a certain identity, ASP. NET will restrict or deny access to resources according to the user's authority.

(4) Secure Communication

Many applications pass confidential data back and forth between end users and intermediate application nodes across the network. Confidential data may include credentials for authentication, or data such as credit card numbers or details of bank transactions. To prevent unwanted information leakage and protect data from illegal modification during transmission, the channels between communication endpoints must be protected.

5.3 Database protection design

This system controls the user's connection to the server through the secure account authentication provided by SQL Server 2000 database management system, and restricts the user's access to the database by using database users and roles. The project management system created different user accounts, roles and granted different rights.

VI. REALIZATION OF SYSTEM SECURITY

According to the business process of project management system, in order to ensure the completeness and confidentiality of information in the whole process of project management, the following security measures must be taken in system design. The project management system uses the ASP. Net application program to carry on the identity authentication through the form. Through this method, the user is guided to a login form provided by the system. Through this form, the user can provide his / her certificate. If he / she is approved, he / she can

Article History: Received: 24 February 2021, Revised: 05 April 2021, Accepted: 08 May 2021, Publication: 30 June 2021

continue the management work. Otherwise, the activity will be cancelled and the page will be relocated to the user login interface. Figure 3 illustrates the form authentication process used in this system.

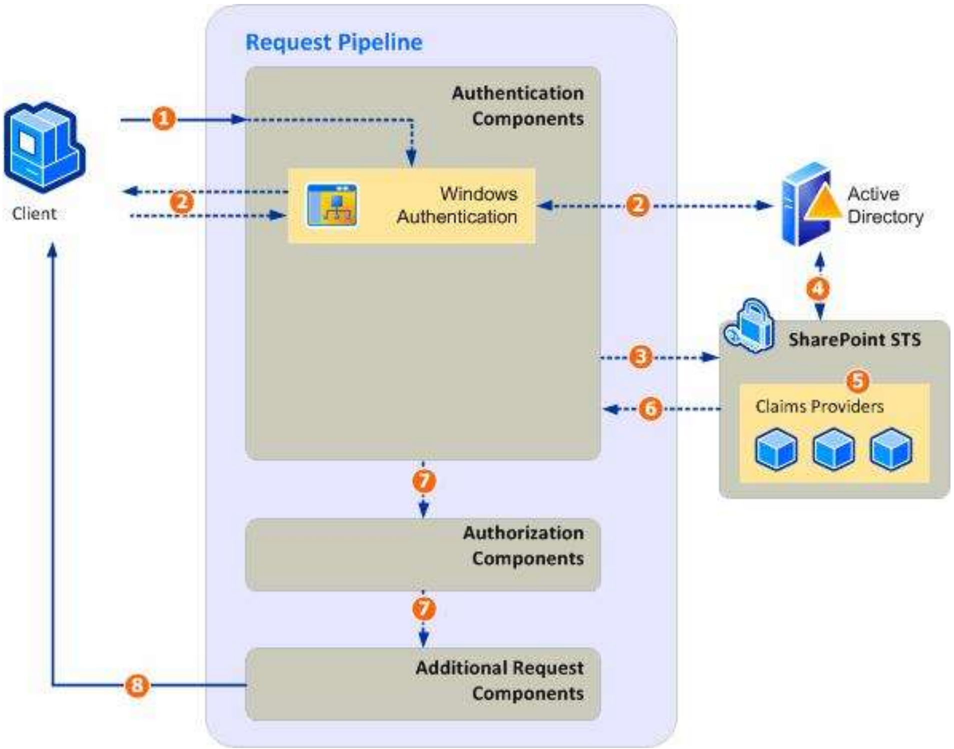


Fig 3: Form authentication process

The steps of the whole process are as follows:

1. The user requests the protected page from the site.

2. If the request does not contain a valid authentication cookie, the web server will redirect the user to the URL specified in the login URL attribute of the authentication tag in the web. Config file, which contains a form for the user to log in.

3. When the user enters the user name and password, the form submits the data.

4. If the input is valid, ASP. Net will create an authentication cookie on the client.

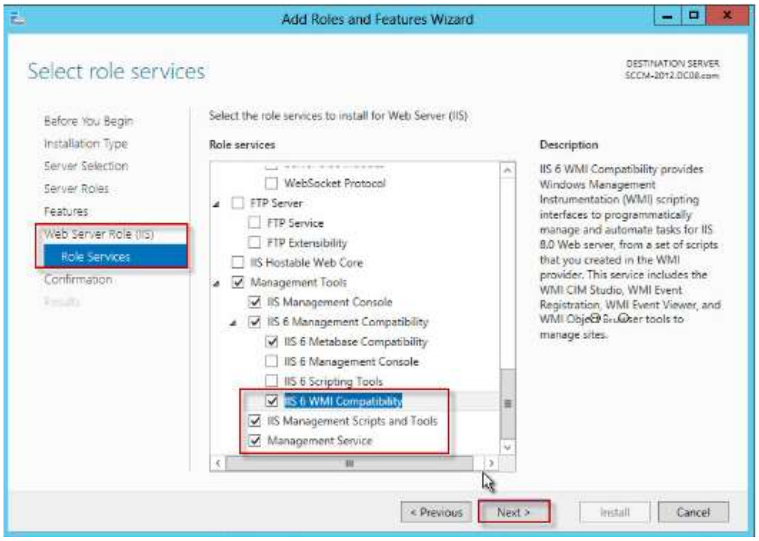
In this way, the user can be redirected to the original request page to continue the management work.

The system uses form authentication with flexible and powerful characteristics. All new page codes will be protected when the system is expanded, and it is not necessary to add protection code for each file. And the authentication process can be customized by the system, and can be added to the authentication policy at will. Through the above safety design, the project management system is more stable, safe and flexible.

If the project management system is connected with the Internet, the security protection of computer operating system is also very fragile because of the considerable security loopholes in the existing network system, and the system will bear huge security risks. Cyber hackers may infiltrate the system, steal data, or maliciously destroy records. Users in the project management system may also disclose the data intentionally or unintentionally. Therefore, the system uses the architecture of the combination of internal and external networks, the internal operation of the project management system is carried out in the LAN, and the external publicity and service are carried out in the Internet.

In this system, each user of the project group has different system roles. The system sets different permissions according to different roles in different project groups. The project manager has the highest authority, and the authority of other users is set by the project management, and can be dynamically modified to meet the needs of project management.

In the project management system, the system administrator endows different roles to the internal personnel of the project management system according to their different identities, and endows them with different permissions for different roles. Because the whole system is divided into different functional modules, so a permission represents the operability of a module or a part of a module. Therefore, each user has the operation authority of the corresponding module according to their role, and is not allowed to operate unauthorized modules. Through this way of authorized access, the project management system will not be illegally accessed and ultra vires operation. Figure 4 shows the system role management.



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
SCCM-2012.DC08.com

Select the role services to install for Web Server (IIS)

Role services

☐ WebSocket Protocol
☐ FTP Server
☐ FTP Service
☐ FTP Extensibility
☐ IIS Hostable Web Core
☑ Management Tools
☑ IIS Management Console
☑ IIS 6 Management Compatibility
☑ IIS 6 Metabase Compatibility
☐ IIS 6 Management Console
☐ IIS 6 Scripting Tools
☑ IIS 6 WMI Compatibility
☑ IIS Management Scripts and Tools
☑ Management Service

Description

IIS 6 WMI Compatibility provides Windows Management Instrumentation (WMI) scripting interfaces to programmatically manage and automate tasks for IIS 8.0 Web server, from a set of scripts that you created in the WMI provider. This service includes the WMI CIM Studio, WMI Event Registration, WMI Event Viewer, and WMI Object Browser tools to manage sites.

Fig 4: System role management

In a word, the system provides a comprehensive management platform for administrators. Administrators can easily manage roles, permissions, etc., while information updating and maintenance are all completed by ordinary users of the system. Through the system and project rights management, we can ensure the security of the system and data at the same time, so that users with different rights can only use the corresponding system functions, browse or maintain the corresponding data.

VII. CONCLUSION

According to the characteristics of Web sites, this paper makes full use of the security in Web.config in. NET and the characteristics of the WEB information publishing system, and adopts the control of the operation rights of directories and specific files to quickly and simply realize different operation rights of different roles. The system provides a comprehensive management platform for administrators, who can conveniently manage roles and permissions, while the information update and maintenance are all done by ordinary users of the system. Through system and project authority management, system security and data security can be guaranteed at the same time, so that users with different authority can only use corresponding system functions, browse or maintain corresponding data. After analyzing the security requirements of the system, this paper introduces two security technologies in detail: access control of backbone role authority and ASP. NET security technology. The application of these two security technologies in this system is realized concretely.

REFERENCES

[1] Bao Xiuguo, Hu Mingzeng, Zhang Hongli. Two Quantitative Analysis Methods for Survivability of Network Security Management Systems. Acta Communication Sinica, 2004, 25 (9): 34-41

[2] Yang Yi, Bian Yuan, Zhang Tianqiao. Network Security Situation Awareness Based on Machine Learning. Computer Science and Application, 2020, 10 (12): 8

[3] Li Zhiyong. Hierarchical Network Security Threat Situation Quantitative Assessment Method. Communication World, 2016, 23: 70-70

[4] Hu Wenji, Xu Mingwei. Analysis of Secure Routing Protocols for Wireless Sensor Networks. Journal of Beijing University of Posts and Telecommunications, 2006, 29 (s1): 107-111

[5] Wei Yonglian, Yi Feng, Feng Dengguo, Yong W, Yifeng L. Network Security Situation Assessment Model Based on Information Fusion. Computer Research and Development, 2009, 46 (3): 353-362

[6] Xu Guoguang, Li Tao, Wang Yifeng. A Network Security Real-time Risk Detection Method Based on Artificial Immune. Computer Engineering, 2005,31 (12): 945-949

[7] Jiang Wei, Fang Binxing, Tian Zhihong. Network Security Evaluation and Optimal Active Defense Based on Attack Defense Game Model. Acta Computer Sinica, 2009, 32 (004): 817-827

[8] Miao Yongqing. Stochastic Model Method and Evaluation Technology of Network Security. China Science and Technology Investment, 2017, 4: 314

[9] Yi Hua Zhou, Wei Min Shi, Wei Ma. Research on Computer Network Security Teaching Mode for Postgraduates Under the Background of New Engineering. Innovation and Practice of Teaching Methods, 2020, 3 (14): 169

[10] Li Weiming, Lei Jie, Dong Jing. an Optimized Real-time Network Security Risk Quantification Method. Acta Computa Sinica, 2009 (04): 793-804