Product Collaborative Design System Access Control Technology on Cloud Manufacturing Services

Dongfang Hu[a], Jianwei Guo[b,*]

[1]School of Mechatronics Engineering, Henan University of Science and Technology, Luoyang 471003, China

[a] hdf@haust.edu.cn, [b] guojianwei1991@yeah.net

Keywords: Cloud manufacturing, Product collaborative design, Access control, System prototype

Abstract: Aimed at the requirement of cloud manufacturing service product cooperating design system access control, the paper proposed a hybrid access control model, which is control model - CMT-RBAC, and gives the model of the operation of the framework and implementation methods based on traditional access control model, role-based access control model and task-based access control model. Developed product design system prototype on the cloud manufacturing service, achieved the high efficient use of simulation analysis of resources, effectively shortened the product development cycle and improved the product market competitiveness.

1. Introduction

Cloud Manufacturing Services Product Collaboration Design System security issues are a central issue in cloud manufacturing service systems. The security function of the product design system of cloud manufacturing service mainly includes identity authentication and access control. For identity authentication, there are a lot of effective, mature implementation methods, such as user / password, multiple password, dynamic time token, SSL, etc. [1-2]. For cloud access service system access control, so far there is no practical, mature model appears. Cloud manufacturing resources are large and heterogeneous, remote, dynamic changes and other characteristics, compared with the traditional access control, cloud manufacturing service environment for resource access control put forward higher requirements.

Cloud manufacturing services is the biggest feature of the service on demand and the efficient use of resources. The existing access control model has autonomous access control, mandatory access control and role-based access control (RBAC). Compared with the first two access control modes, RBAC model is more suitable for commercial use [3-4]. RBAC through the role of users and permissions to establish contact between, and some of the constraints and inheritance mechanism cited, thereby enhancing the use of security permissions, reducing the difficulty of the management of authorized work. However, if it is directly applied to the cloud manufacturing service system, there are some shortcomings of its own: on the one hand, the role of RBAC in the authorization is often static, can’t be well adapted to the cloud manufacturing system dynamic service needs; Aspects, in the RBAC, the role of a distribution with the characteristics of life, there is no good role to eliminate the mechanism. It will has a certain amount of power waste, and can’t meet the requirements of the system on demand services. Therefore, the establishment of cloud access service for the access control model is a cloud manufacturing service system to achieve a difficult and key points.

2. Traditional Access Control

2.1. Access Control Technology

Access control (AC) is to prevent the intrusion of illegal users or legitimate users of the improper operation of the system caused by the destruction of key resources, through a certain way to limit the main access and access to the scope, and then achieve a safe access to resources strategy. In recent years, most of the research on access control has been carried out around some access control models [5-7]. Subject, object, and access control strategy are the three elements of the access control model. Access control is a process in which the subject performs access to the object. The basic principle is shown in Figure 1.

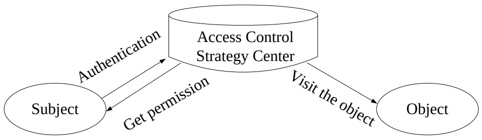

Figure 1 Access control principle

Authentication is the first step in the subject's access to the object. When the authentication of the subject is passed, the corresponding access to the object is obtained in order to access the object objectively. For an unlawful subject, it is denied access by the Access Control Policy Center, can’t gain access to the object, and prevents unauthorized users from accessing the object, thus ensuring the security of the system in terms of access control.

2.2. Autonomous access control

This access control is called Discretionary Access Control (DAC) if the owner of the object (owner) can grant or deny access to the object by accessing the attribute's settings. In the DAC, the object's access control authority is in the hands of the owner. Its main feature is the autonomy of the main body is relatively large, the main body can own access to other subjects have access to other subjects, regardless of whether the system allows. Permission management is a common problem in the process of access control. In the autonomous access control system, the access control list or the access control matrix is widely used to realize the specific authority control.

2.3. Role-based access control

Role-based access control, user (User), role (Role), permissions (Permission) is the three most basic concepts. Role is the core of RBAC, access is no longer directly granted to the user, but with the corresponding role associated with the role given to the corresponding user. In the RBAC model, through the introduction of the concept of role to achieve a relatively stable authorization, the basic realization of the principle shown in Figure 2.

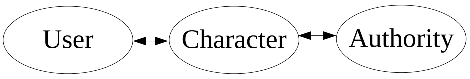

Figure 2 RBAC basic principles.

When the RBAC system is running, the system administrator first authorizes the different roles. Once the role of the authorization process is completed, then the role of the corresponding permissions will no longer change. Each role can be associated with one or more entity (subject or object) permissions, and each user can have one or more roles at the same time. In the RBAC system, the user through the session to activate the corresponding role in order to obtain operational authority.

2.4. Task-based access control

The basic idea of TBAC is to determine the grant of authority according to the running state of the task. When the state of the task changes, the user's authority changes accordingly. In other words, the user's authority is no longer static, with the task needs to increase or decrease. For the workflow system, each step of the data processing is related to the previous step. Because the user's task in the workflow is time-limited, so the user's permissions are also time-limited, when the task is completed when the corresponding authority will be the system to recover. TBAC operating principle shown in Figure 3.

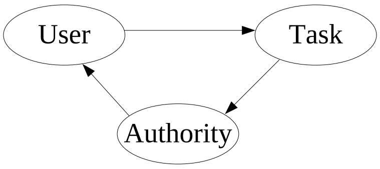

Figure 3 TBAC operating principle.

Users in the implementation of the workflow process, each step task has the corresponding operating authority, the system will be given the authority of the dynamic users to meet the needs of the task operations. When a task is over, the task corresponding to the authority will be recovered by the system, the system automatically transferred to the next task state, and then give the user the appropriate authority again, so repeated authorization, until the end of the entire task flow.

3. Collaborative Design System Access Control Model for Cloud Manufacturing Services

3.1. Access Control Model

The Collaborative Design Access Control Model (CMT-RBAC) of cloud manufacturing services is based on the RBAC97 model, which extends the concept of task flow in TBAC. The CMT-RBAC model completely inherits the concept of the RBAC97 model, and divides the authorization in the TBAC model into static authorization and dynamic authorization. The static authorization is associated with the role, and the dynamic authorization is associated with the task, thus realizing the two models of RBAC and TBAC (CMT-RBAC), as shown in Figure 4.

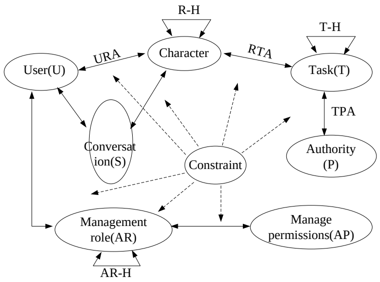

Figure 4 CMT-RBAC model.

In the CMT-RBAC model, the participating users of the collaborative design task process will be assigned the specified role, and then specify the range of tasks and minimum permissions that each role can perform. As can be seen from the structure of the model, the user's rights are no longer directly related to the role, but must be through the corresponding task to be associated with the role. In the access control system built by CMT-RBAC, the user can log in to the system through the administrator's pre-assigned role, but at this time the user does not have the access rights of the resource. The user must obtain the access right of the corresponding resource through the task process of the system assignment. When the task execution ends, the user's authority is automatically reclaimed, thus realizing the dynamic allocation and management of the authority and improving the dynamic adaptability of the system.

3.2. CMT-RBAC Model Operation Framework

The operation function of CMT-RBAC model mainly includes two parts: access control and application service execution. The access control server is the core part of CMT-RBAC model operation. It is also composed of three sub-parts of authentication module, role management module and task privilege management module, the corresponding by the authentication server, role management server. The task rights management server to implement specific operations. CMT-RBAC model specific operational framework shown in Figure 5.

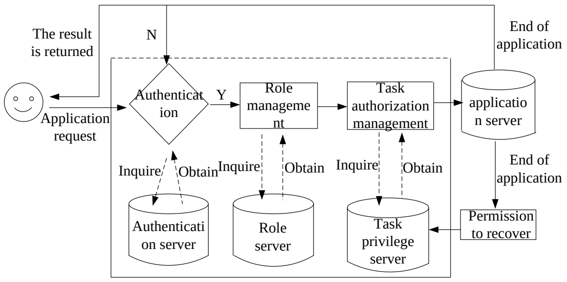

Figure 5 CMT-RBAC model operational framework.

3.3. Implementation of CMT-RBAC Model

Role division. The rational division of the role is to achieve the basis of effective management of authority, is to reduce the access control process of the system authorized workload, improve the system's operating efficiency of the premise. For the role of the size of the division, to control in a moderate range, if the role of the granularity of the division is too small, will lead to overlapping roles between the role, will increase the system's rights management difficulty, not to simplify the purpose of authorization; The granularity of the division is too coarse, and the role of the role is too centralized, not suitable for the assignment of roles, which not only lead to the waste of authority, but also increase the risk of access control of resources in the system, contrary to the use of the role to achieve efficient and safe Access to the original intention of the system resources.

Authorization process. Authorization is a process of authority. The CMT-RBAC model system's authorization consists of two parts: static and dynamic.

Constraint management. In the collaborative design system of cloud manufacturing service, with the collaborative design task, there will be some conflicts, such as role conflict, task conflict, the authority conflict and so on. The introduction of constraints is to avoid the user in the process of resource access to the conflict, so that only the binding operation was allowed to implement, to ensure the smooth development of the design task. The constraints in the CMT-RBAC model mainly include role constraints, task constraints and authority constraints.

4. Conclusion

This paper introduces the basic principles and concepts of access control. On this basis, traditional access control (MAC and DAC), role-based access control (RBAC), task-based access control (TBAC) are introduced, and their respective Advantages and disadvantages of the analysis and comparison. Based on the RBAC97 model, a collaborative design system access control model (CMT-RBAC model) for cloud manufacturing service is established by introducing a task-based access mechanism based on the characteristics of access control of collaborative design system of cloud manufacturing service. Finally, the operation framework of CMT-RBAC model is given, and the concrete implementation of the model is studied.

Acknowledgements

The author is very grateful to the National Natural Science Foundation of China(No. 51475142). Henan Provincial Department of Education Natural Science Research Project (Project No. 12B520019), and the Major and previous pre-research project of Henan University of Science and Technology (Project No. 2011CX016).

References

[1] Liang Ce, Xiao Tianyuan, Zhang Linxuan. Access control for collaborative environment in networked manufacturing system[J]. Computer Integrated Manufacturing Systems, 2007, 13(1): 136-140+152.

[2] Cai Hongxia, Yu Tao, Fang Minglun. Access control of manufacturing grid[J]. Computer

Integrated Manufacturing Systems, 2007, 13(4): 716-720.

[3] Cai Meisong. Rbac based policy research and collaborated aerospace product development platform application[D]. Shang Hai: Shanghai Jiaotong University, 2007, 04: 20-35.

[4] Du Ping. Application research of role based access control for computer supported cooperative work in design[D]. Ji Nan: Shandong Normal University, 2007, 04: 2-8.

[5] Gu Chunhua, Xiao Baoliang. Role permission in hierarchy relation of RBAC model[J]. Journal of East China University of Science and Technology(Natural Science Edition), 2007, 33(1): 96-99.

[6] Hong Fan, He Xubin, Xu Zhiyong. Role-based access control[J]. Journal of Chinese Computer Systems, 2000, 21(2): 198-200.

[7] Fu Ximei. Access control strategy based on RBAC in collaborative environment[J]. Computer Engineering, 2009, 35(11): 140-142.