A Flexible Workflow Model of Role Based Access Control

Jianmin Zhao[1, 2, a], Jian Kang[2, b] and Tiange Li[3, c]

[1]State Key Laboratory of Enhanced Oil Recovery, Beijing 100083, China

[2]School of computer technology, Northeast Petroleum University, Daqing 163318, China

[3]DaQing Oilfield of CNPC, Daqing 163318, China

[a]zjmde@126.com, [b]kangjiandeyouxiang@163.com, [c]tlitg@petrochina.com.cn

Abstract. For the shortcomings of the traditional workflow in flexibility, this paper analyzes the advantages of Role Based Access Control Technology (RBAC) in realizing procedure permission dynamic management. With RBAC applied in it, this paper also constructs the flexible workflow model of Role Based Access Control and gives out the definition of the engine as well as the components concerned. In addition, it also solves the problems of the flexible operation of resource and dynamic assigning tasks in the business process, and applies the engine into the specific business process.

Keywords: Workflow, RBAC, Flexible, Permission.

1. Introduction

Workflow is the computerization and automation of the business process, with the help of computer, it changes the work patterns in the traditional business process, makes the process continue automatically, safely and methodically so as to achieve the expected business objectives [1]. This style is fit for the inherent working process, however, as for the workflow system, there comes many more challenges by the fining and complexity in the business process in the modern cooperation, so the disadvantages of the traditional workflow system becomes increasingly salient. Enterprises need flexibility, and flexible workflow system has become the newly hot pot in the field of enterprises and researches. A role based access control flexible workflow model is presented in this paper [2]. It analyzes how to realize the dynamic authorization relations of users, roles and permissions. Under the constraint conditions such as the least permissions and separation of duties, valid users can come in at the right time so as to realize the flexible operation on the process object and ascertain the process instance to go on smoothly.

2. RELATED CONCEPTS

RBAC: Role Based Access Control. *RBAC* model includes users' role assignment, permission distribution based on role and the inheritance relation among the roles.

Workflow: According to the definition of Workflow Management Coalition (*WFMC*), workflow means to realize part or the whole business process with the use of computer, and in terms of series of rules in the process, documents, information or tasks can be automatically delivered, carried out among different executors.

Flexible workflow: 'Flexible' means that an object can try to protect its shape from being changed when influenced by outer force and it has a comparatively good adaptability [3].

3. The Analysis and Design of the Flexible Workflow Based-on Role Based Access Control

3.1 The Inevitability Produced by the Flexible Workflow system.

Workflow, created in the 70s in last century and experienced tens of years' development, has been applied into all trades and professions from its initial application of *OA* (Office Automation). With its

application deep-going and expanding continuously, there raises some higher requirements for workflow. A very important thing is the flexibility and dynamicity of the workflow system. Most of the traditional workflow systems are static and cured; some sections such as process modeling, customization as well as run of instances are lack of flexibility and adaptation, however, our modern society is dynamic, business process often change, so it is necessary for workflow system to be provided with the ability to react to some unexpected changes and keep itself in the normal condition. Flexible workflow is raised just based on the flexibility and dynamicity; it can describe the dynamic process of enterprises more accurately and meet the actual need of enterprises [4].

3.2 RBAC Technology

Role Based Access Control technology(*RBAC*), with high security and flexibility, is raised as a subject-object access control technology considering that Autonomy Access Control (*DAC*) is not safe enough and Media Access Control (*MAC*) is not flexible enough. Introducing the concept of 'Role' between the executors of different tasks, according to the Many-to-Many possession-related relationship between roles and permissions, the Many-to-Many assignment-related relationship between users and roles, depart users from the tasks for process and reduce the degree of coupling, so any aspect changes will not cause a huge fluctuation of the other ones[4].

RBAC model includes *RBAC0, RBAC1, RBAC2, RBAC3* four basic modules, Complete *RBAC* model shown in Figure 1:
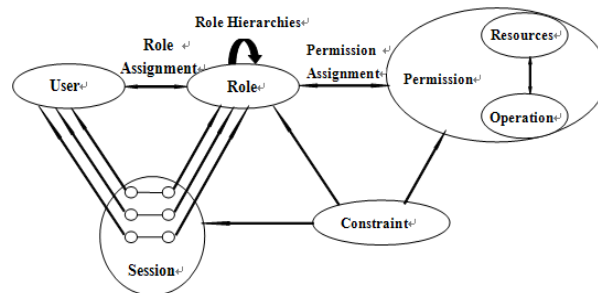

Figure1. RBAC model

RBAC model includes the collection of some main entities:

- User set: The actual task executor of process generally refers to human.
- Role set: role is an abstract conception, Consider users' job function as well as the permissions that they have when operating on the resources and get out the concept of roles.
- Permission set: Permission is a two-tuples including operation and resource. The subject can hold different operations of different resources while he possesses some certain permission.
- Session set: A session is established when a Dynamic activation happened between the user and his related legitimate role. Session and the static role-user assigned relationship are different.
- Constrain set: Constraint is a series of restrictive conditions existed among the entities of the *RBAC* model. Some certain conditions of the constraint set must be satisfied in the access control in order to ensure safety, legality, flexibility, and accuracy of the access control.

3.3 Flexible Workflow Model of Role Based Access Control

a) The raise of model

Workflow model, raised by *WFWC*, includes six component parts and five interfaces. The relation between workflow production server and workflow client application manifests the distribution between tasks and the task executors. Both of them connect each other by one interface. The process instance based-on this model has much inflexibility. However, the flexible workflow model, based on roles and relies on RBAC technology, constructs an independent user permission management, which is specifically used to manage the relation among users, roles and permissions in the business process. Between the workflow production server and workflow client application program inserts a user permission management model can make them two have a logical subroutine call relation, but when actual workflow works, it will set up a mapping relation between the workflow task and permissions, task executors and user, according to the user permission management model, so as to realize the dynamic distribution from workflow task to task executors, as shown in Figure 2.
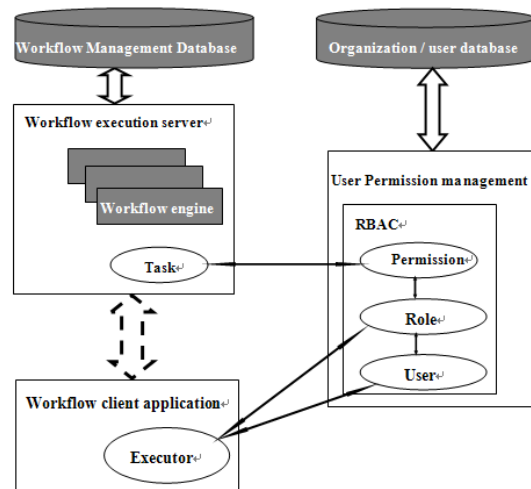
Figure2. Flexible Workflow Model Of Role Based Access Control

b) The Definition of Formalization of model element

The definition of formalization of model elements based-on the model above is as follow:

Workflow tasks (TASKS, shortly recorded as *T*) maps the permission in user permissions management model (Permissions, shortly recorded as *P*); workflow client task executor (*E*) maps Roles *R*, Users *U* in the user permission management.

Workflow Engine defined Process Tasks: to achieve the mapping of every Element T of sets of Process tasks and permissions $P = \{P1, P2,......PN \mid Pi = \{(REi, OPi) \mid i = 1,2,......N\}\}$ of the user rights management model.

User permission management model realize the distribution of Permission P-Role $R: PR \in P \times R$, and Role *R* possesses the Permission *P*, $ROLES(P) = \{p \in P \cap (p, r) \in PR\}$.

User permission management model realized the distribution of Role R-User U: $RU \in R \times U$, and User U possesses the Role R , $USERS(R) = \{r \in R \cap (r, u) \in RU\}$.

The task executor *E* can be a certain user, but specific users cannot be determined at the time of process definition. Task executor (E) map to a kind of roles R, then executors can be any accessible members who possesses the $R, E = \{(u \cup r) \mid u \in U, r \in R\}$.

Least Permission Constraint: The Many- to-Many relations between users and roles, roles and permissions determine that users can be endowed with much permission relevant to the roles. When realizing the task distribution in real process, users have the least permission (u) needed for finishing the tasks, that is to say, the completed tasks carried out by the minimum operation on the object resource . Compared with the simple tasks, users only need to activate a legal role but don't have to activate all the permission related to the role. Complex tasks need more roles and the permissions relevant to complete. Define two marking variables Fr and Rp to judge whether each role and the permission related have been activated [5].

4. Case Analysis of application

The engine constructed based-on above, adopts the program of *c#*, and then package the engine after developed to be a dynamic link library, and put it into practical application. Figure 3 shows workflow of examination and approval of newspaper articles, including draft, proofreading, check draft, competent reviewer, modify draft, and dispatch the six basic steps. In flexible role-based access control workflow system, staffs of the organize as a starting point; choose some most appropriate staff in all the working procedure. And give a certain permission to them to finish the assigned task. That different participant in the draft and manuscript itself is bound to cause different process instance. Proofreading, check draft, competent reviewers, each procedure will affect the choice of the executive in the next procedure. Users with different recognitions and opinions on the draft make different decisions, so the execution path in the approval process will be different. Process execution should

correspond to the above analysis of various constraints in the definition and creation so as to ensure that each flow can complete legally, flexibly and efficiently.
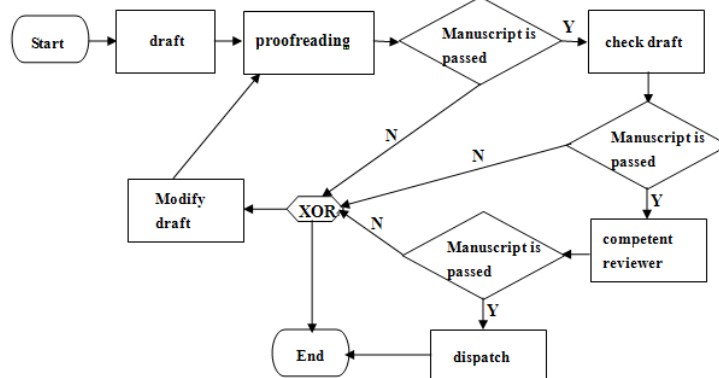

Figure3. Examination and approval of newspaper article

5. Conclusion

Flexible workflow has been the hottest point of research in the field of workflow. This paper constructs the workflow engine based on the Role Based Access Control and realizes the dynamic authorization relations of Users- Roles-Permission. Under the constraints such as the least privileges and separation of duties, valid users can be the legitimate role at the right time so as to achieve the flexible operation on the flow object resource and ensure the process instance successful implementation. It constructs user security control model, monitors and manages the flexible distribution of the personal privilege in the business process. The author will do further researches on flexible workflow based on the roles, through the examples that are more widely used to make adjustments, improve flexibility of the workflow system, better meet the needs of enterprises while developing.

Acknowledgments

References

[1] David Hollingsworth. Workflow Management Coalition the Workflow Reference Model [M].TC00-1003.HamPshireUK:2002, 4~50.
[2] WEBER B, RERCHERT M, RINDERLE S. Change patterns and change support features-enhancing flexibility in process-aware information systems [J]. Data and Knowledge Engineering 2010, 66(3):438~466.
[3] Mavridis I., Georgiadis C., and Pangolins G., Khair M.: "Access Control based on Attribute Certificates for Medical Intranet Applications". Journal of Medical Internet Research (JMIR) 2011:3(1):e9.
[4] Abraham Bernstein. How can cooperative work tools support dynamic group process? Bridging the specificity frontier. The 2000 ACM conference on Computer supported cooperative work[C]. Philadelphia, Pennsylvania, United States, 2009:279~288.
[5] ZHOU Jian-tao, SHI Mei-lin, YE Xin-ming State of arts & trends on flexible workflow technology. Computer Integer and Manufacturing Systems 2012 11(11):1501~1510.