Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(2):101-109

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Researches on the access secure control workflow model based on role

Zhai Jinbiao

State Key Laboratory of Software Development Environment, School of Computer Science and Engineering, Bei Hang University, China

---

ABSTRACT

With the rapid development of innovative computer technology, the computing environment of the workflow has become distributed and heterogeneous. Security management of WMS becomes weak. And the possibility of security leak will increased. The important information and the data are threatened more and more seriously. The security problem of workflow has become the hot spot in current research institutions and organizations concerned. Role-based access control model (RBAC) simplifies the permit management. It also reflects the access control mechanism in the organization and the enterprises. So the RBAC is very popular to design the workflow. In this paper, we present the multi access control security model based on roles. We propose the implicit and explicit authority management based on the roles. These measures enforce the security of this mode in computer environment. The first part of this paper is the introduction of the related problem. The second part is the concept of access control based on role. The third part is the multi access control security model based on roles. Then, the final part is the authority management.

Key words: Workflow, RBAC, Security, Permission

INTRODUCTION

Workflow management system is an apply software generated for workflow. With the development of workflow technology, computer technology, network technology, database technology and workflow management system has been widely used in manufacturing, commodity circulation, financial management, office automation and other areas. The workflow management system provides efficient and flexible process management for the above areas [1-3]. On the one hand, the research on workflow management system is more and more in-depth. People are increasingly dependent on the business process of workflow management systems. On the other hand, workflow management system has been exposed more and more information security problems which make people have to consider whether to use the workflow management system [4]. Therefore, the information security problem of workflow management system has become a major problem in academic and industrial circles.

In 1998, WFMC released the workflow security white paper. In this paper, the organization divides the security of workflow into eight aspects: authentication, authorization, access control, audit, data privacy, data integrity, non-repudiation and safety management [5]. So far, many scholars have studied on the access control problems. They put forward some access control models, such as the Discretionary Access Control (DAC) [6, 7], Mandatory Access Control (MAC) [8-9], Task-based Access Control Model [10], Role-based Access Control Model and RBAC [11-14] etc. The basic idea of the DAC model is that using the access control list (ACL) to describe the access permission relationship between interviewed object and subject directly [8]. DAC is easy to use, but it has low flexibility. It can't adapt to the workflow management of user authority transfer, because there is no intermediary between the subject and the object. MAC model defines the object security level firstly. Then, it strengthens the special protection safety level of the object by the classification management of access permission. At the same time, it lacks the flexibility of authorization. Therefore, the MAC model can't also adapt to the workflow management of

user authority transfer [9]. The TBAC model is no longer to set permission in the workflow management for the surveyed object. But it asks for authorization in the business process and associates the various entities in access control. The TBAC model is able to express the business process execution between steps and access control clearly. But the user's visual figure is not intuitive in access control. The TBAC model lacks the transfer of user support because it can't express the relations directly between task and user authorization. The RBAC model takes the role as a user and interviews object between media and assign that through a role to object and user to role to realize the two phase authorization. In the RBAC model, roles can represent the positions or departments. The user can even be individuals or groups [11]. The RBAC model has become the authorization mechanism of workflow management in natural selection [12]. Many scholars research the workflow access control model based on role. In 1992, Ferraiolo and Kuhn proposed the role access control based on this concept firstly [13]. Then, the domestic and foreign scholars have done a lot of researches on the RBAC model, especially for the RBAC model in a workflow management system. In 1996, Sandhu proposed the RBAC96 model. Bertino and Ferrari proposed authorization constraint language in a workflow management system based on role in 1999[14].Botha and Eloff summed up the four separation demands: role conflict, conflict license, user conflict and task conflict [15]. With the continuous deepening research of mobile agent technology [16], Cichocki et al put forward the concept of migrating workflow in 1999 [17-18]. This concept soon became a new direction of workflow research. Working place provides the run-time service and workflow services, such as immigration, emigration, authentication, authorization, communication, data access and programs etc. Scholars research migrating workflow modeling [19-21]. For example, migrating instance routing [22], working position of active [23] and the communication mechanism of migrating workflow [24].

Based on the above model, this paper proposes a new role based on access control model of multi-layer safety aiming at the safety problem of workflow. And this workflow is based on the role. Its authorized management is studied. We put forward the concept of DcAC to manage and task the related documentation. The workflow model has characteristics of authorized management centralized, policy neutral and security high granularity. It also supports the principle of least privilege and separation of duty.

ACCESS CONTROL MODEL BASED ON ROLE

The basic idea of the access control model bases on role (RBAC) which is the set of permission. The user obtains permissions through roles assignment. Then, the system can achieve or change the control strategy though the multi to multi assignment among user, role and permission.

RBAC includes three parts: user, role and permission. The user is the subject to operate on the data object. It can be personal, computer or robot. A role is a task or job title within the scope of organizations. It represents the task category specific. Permission is the access license to the objects in the system. It is similar to the concept of "insert, delete, change" in the system.

The entity relationship of RBAC is showed in figure 1

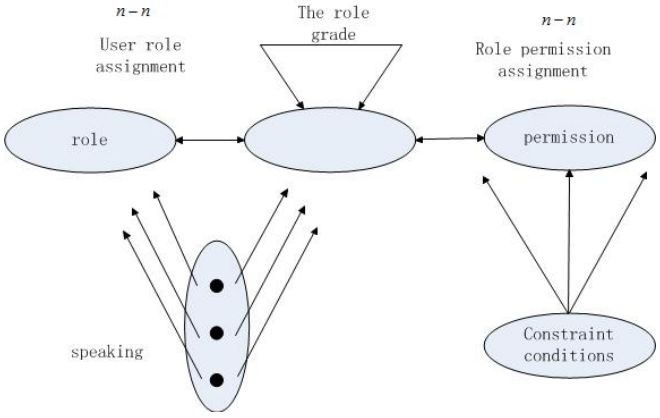

Figure.1 The entity relationship of RBAC

The RBAC96 model consists of four sub models: RBAC0, RBAC1, RBAC2 and RBAC3.RBAC0 is the basic mode.RBAC1 introduces the concept of role hierarchy on the basis RBAC0. RBAC2 introduces some constraints on the basis of RBACO.RBAC3 is the organic combination of the first three models.

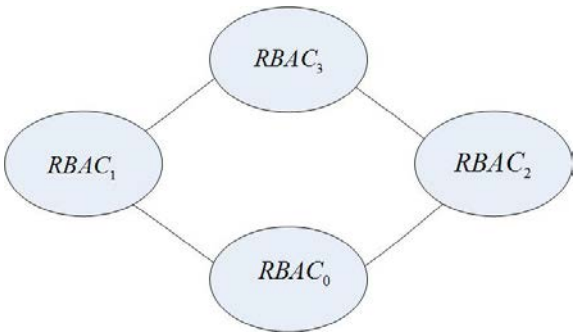

Figure.2 Schematic diagram of RBAC96 model

Definition:

(1) (U, R, P, S) (user, role, permission, speak)

(2) $PA \subseteq P \times P$ (permission assignment, many to many relationship)

(3) $RH \subseteq R \times R$ (A partial ordering relation of role relationship or role levels, express as $\geq$)

(4) $Roles : S \rightarrow 2^R$

MULTI ACCESS CONTROL SECURITY MODEL BASED ON ROLES

As we all know, a workflow is consisted of many tasks which can complete the functions. Because these tasks contact each other, they complete the functions in a cooperative way. The related workflow permission mechanism should be reflected in a workflow management system to make sure that the tasks can be executed within the specified time.

A workflow can be composed of multi-layers. The whole system can be expressed as the integration of different levels. Interactions between two tiers are triggered by events and management. Monitoring between different layers is authorized by each layer.

In this paper, the security model is based on the concept of role. The workflows are authorized by each layer.

3.1 The basic definition of elements

The basic elements involve in the multi access control security model based on the roles are:

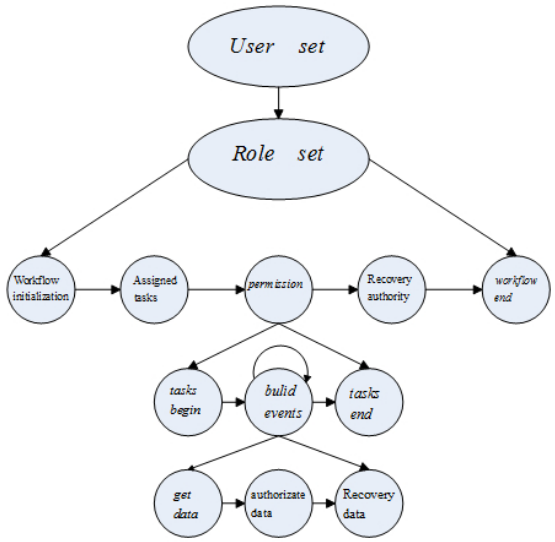

Figure.3 security control model

When the workflow definition is in the process of executing, it needs to transfer the documents, information and tasks among the participants according to some rules. When RBAC is combined with workflow, we must consider how to handle the relationship among documents, tasks and roles. Now we introduce the security workflow model which is based on RBAC. This model will focus on the right management among these three aspects. It strengthens

the management on the part of the document authority. Permission divides into the display management and the implicit management. Besides, we definite the concepts of DcAC, EP, EPA and IPA.

The entities in the model include role, user, permission, constraint, task, task instance, document access control specification, document and session. Their definition, representation and related functions are as following:

(1)R:The role set corresponds to the position or the job in the organization. It can be an abstract concept. It can also be the position and rights corresponding to the specific application fields.

(2)U:The user set is the main subject to visit the data resource in the computer system. It can be a person or an intelligent agent.

(3)P:The permission set is an abstract description about the permissions which the tasks have. It can be expressed as the set about an object(O) and the operation(P). $P = O \times OP = \{(o, op)\}$

(4)C:The permission constraint set can apply to every entity and relation in a model. It can achieve the higher level security management strategies such as the separation of duties.

(5)T:The task set is the smallest unit which can be distinguished in the workflow.

(6)TI: The task instance set is a specific task execution. A task can correspond to multiple instances according to a different context. Therefore, it exists one to many mapping. We call it as the instance mapping. It is as following: $M : T \mapsto TI$ .The definition corresponds to all instances set in a task. For example, $M(t_j) = \{ti_1, ti_2, \cdots\cdots, ti_m\}$ means that there are m task instances correspond to the task t_j .

(7)D:The document set is the existence form of the data in the model.

(8)DcAC: It is document access control instructions set and manages the documents which are related to tasks. It also manages the operations about the documents. DcAC is the set about the documents and the operations. It is corresponding to the task and represents the operation permissions and the access sequence that the tasks have. This set can be expressed as following: $DcAC = \{(d, op)\} \in D \times OP \in P$ .There are two mapping among the tasks, documents and Dcac: $F(\exp licit \quad dcac \quad mapping)$ and $G(\exp licit \quad document \quad permission \quad assignment)$.

① $F : T \mapsto DcAC$:It defines a one-to-one mapping between the task and DcAC such as $F(t_i) = dcac_i$ .When any instance is running in the task, the corresponding DcAC will be instantiated with the instance.

② $G : DcAC \mapsto D \times OP$:It defines the set about documents and operations which the DcAC contains. For example: $G(dcac_j) = \{(d_{j1}, op_{j1}), (d_{j2}, op_{j2}), \cdots, (d_{jk}, op_{jk})\}$.

We can get the combined function $F \circ G : T \mapsto D \times OP$ according to the definition between F and G. We can know $D \times OP \in P$ according to the definition of permission (P).Therefore, DcAC is equivalent to the intermediary between the task T and the permission P. It authorizes the management of documents. It eases the workload and enhances the authorization management model.

(9)S: The session set is a span. It corresponds one-to-one to the user and the task instance. They have a mapping relationship as the following:

① $SI : S \mapsto TI$ .It defines the one-to-one mapping between the session and the task instance. $\forall s \in S, ti \in TI, SI(s) = ti$.

② $SU : S \mapsto U$ .It defines the one-to-one mapping between the session and the user. $\forall s \in S, u \in U, SU(s) = u$.

(10)E: The set of events. Events are the sign of trigging the beginning and the end of the tasks in workflow.

(11)TAC: Tasks accessibility control. This means the required conditions to complete tasks.

3.2 Definition of the relations between elements

(1) $PR: D \to P$ is the permissions which are obtained from documents and data. $PR(d_i) = \{pi_1, pi_2, \cdots, pi_n\}$ is the permissions $pi_1, pi_2, \cdots, pi_n$ obtained from documents and data d_i Generally speaking, $PR(d_i) \subseteq p$.

(2) $F: T \to TAC$ is a map controlled by each task. It is the accessibility of the corresponding task.

(3) $G: TAC \to DxPR$ is a pair of the permissions controlled by accessibility of the corresponding task from the documents and data.

(4) $PT: P \to T$ is the task of the permissions.

(5) $US: (u: user) \to 2^{RS}$ is a reflect from the user sets to role sets.

3.3 Permission process

The permission process in this model is that system authorizes during task execution when calling a task or cancelling a task and the permissions of the data related in task. Function $timestamp()$ is integral expression of the current time.

Definition 1: This model assigns corresponding tasks to each role to make sure the correctness of the authorized

$Assign(t, r)$

$if \quad t \in T \quad and \quad r \in R\{$

$if \quad t \in F(t)\{t \to r\}$

}

Definition 2: This model assigns corresponding permission to each role to make sure the authorized integrity

$GrantT(t, p)$

$if \quad t \in T \quad and \quad p \in P\{$

$assign(t, r)$

$granted(t, timestamp())$

}

}

Definition 3: This model will take back the permission of the tasks after the tasks are over to make sure the authorized integrity.

$\mathrm{Re}vokeT(t, p, r)$

$if \quad t \in T \quad and \quad p \in P \quad and \quad r \in R\{$

$for \quad all \quad granted(t, p, timestamp())\{$

$revoked(t, p, timestamp());$

}

$granted(t, timestamp())$

}

}

Definition 4: This model will generate the events in the tasks to make sure the authorized integrity.

$GenerateE(t, e)$

$if \quad t \in T \quad and \quad e \in E\{$

$generated(e, timestamp())$

}

Definition 5: This model will authorize control conditions to the documents and data in execution time to make sure the authorized integrity.

$GrantD(t,d,p)$
$if \quad t \in T \quad and \quad e \in E \quad and \quad p \in P\{$
$if \quad exist(granted(t,p)) \quad and \quad not \quad revoke(t,p,r)\{$
$granted(d,p,timestamp());$
}
}

Definition 6: This model will take back the permission of the documents and data after the tasks are over to make sure the authorized integrity.

$\mathrm{Re}vokeD(t,d,p)$
$if \quad t \in T \quad and \quad d \in D \quad and \quad p \in P\{$
$if \quad exist(granted(d,p)) \quad and \quad not \quad revoke(d,p,r)\{$
$if \quad \exp ired(timestamp())\{$
$revoked(d,p,timestamp());$
}
}
}

PERMISSION MANAGEMENT

Although the multi-level security control model can improve the safety of the model, there are still some loopholes in the authorization process. We present explicit permission and implicit permission to strengthen the security of model.

Explicit permission (EP) is the link between the task set and the set of operations. The EP is assigned to a role and this relationship is called explicit permission assignment (EPA).

Implicit permissions (IP) is the link between the task instance and the set of operations. If a task is assigned to a role, then all task instances which are associated with the task are assigned to the role. This is called implicit permission assignment (IPA).

4.1 The Permission Relation in the Model

Kandala and Sandhu put forward the explicit permission, explicit permission assignment, implicit permission and implicit permission assignment in the literature. The model uses a similar but different definition to explain the permission of the model.

(1)Explicit Permission (EP): The set of two-tuples (o,op).The subject object is the role while the object is the task and the document in the model. EP is divided into $TEP(\exp licit \quad permission \quad on \quad task)$ and $DEP(\exp icit \quad permission \quad on \quad document)$. Therefore, $EP = TEP \cup DEP \subseteq O \times OP$.

(2)Explicit Permission Assignment (EPA): It assigns EP to roles. That is, $EPA = EP \times R$.

(3)Implicit Permission (IP): It is the permission which relates to the instances. It also includes TIP and DIP. Therefore, $IP = TIP \cup DIP \subseteq O \times OP$.

(4)Implicit Permission Assignment (IPA): It assigns IP to the roles. That is, $IPA = IP \times R$.IPA is completed according to EPA.

We need to achieve two part authority managements in the model.

(1)One person operates the document which he owns. It means that any instances own the same operations to these documents in a task.

(2)The role operates the task execution. The role has the same operation for every instance in the task. In this paper, the subject of the model is the roles while the object of the model is tasks and documents. Among them, the roles

and tasks are direct association. The tasks and the documents are association directly. Roles associate with the documents according to the tasks. Roles have different operations between the tasks and the documents. For example, the roles may have the operation of the tasks $TOP = \{execute, commit, abort\}$ .The roles may have the operation to the documents: $DOP = \{read, write, read / write\}$ .We separate the two part operation. We introduce the entity DcAC. It is used to manage the operations of the documents which are related to the tasks. According to the previous DcAC and the definition of the permission, the content of the DcAC is actually a part of the permission (P).Because of the one-to-one relationship between the task and DcAC, we can take the DcAC and the permission which related to the task as a whole $DcAC \cup TEP$ .That is, we assign the EP to the roles. We call it EPA. We regard the DcAC and the tasks as a whole. A task may include multiple instances. Therefore, every DcAC can link a task instance. If a role has the permission to execute a task and a related document, the role will have the same permission to any instances of the task. That is IPA. We achieve the above two parts of the authority management through these mechanisms.

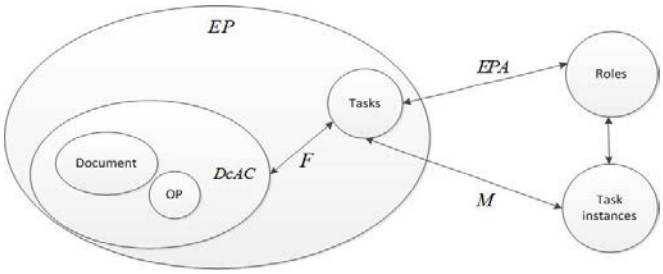

Figure.4 The model authorization management pattern

5.4 The Formal Description and the Graphical Representation

(1)The model entities include: the role set(R),the user set(U),the permission set(P),the constraint set(C),the task set(T),the task instance set(TI),the document access control set(DcAC),the document set(D) and the session set(S).

(2) $RH \in R \times R$ is called as the role hierarchy. It is a partially ordered set about the roles. It can be expressed by $\prec$.

(3) $UA \subseteq U \times R(User \quad Assignment)$

(4) $OP = DOP \cup TOP$

(5) $TEP = TOP \times T$

(6) $DEP = DOP \times D \times T = DcAC \times T$

(7) $EP = TEP \times DEP = TOP \times DcAC \times T$

(8) $TIP = TOP \times TI$

(9) $DIP = DOP \times D \times TI = DcAC \times TI$

(10) $IP = TIP \times DIP = TOP \times DcAC \times TI = \{(op, dcac, t_i) \mid \exists[(op, dcac, t) \in EP] \wedge t_i \in M(t)\}$

(11) $P = EP \cup IP$

(12) $EPA \subseteq EP \times R$

(13) $IPA = IP \times R = \{(r_i, op, dcac, t_i) \mid \exists[(r_i, op, dcac, t) \in EPA] \wedge t_i \in M(t)\}$

(14) $PA(permission \quad assignment) = EPA \cup IPA$

(15) $permission : R \mapsto 2^{IP}$ .It defines the mapping between the role and the permission. If there exist the role

hierarchy, the mapping between roles and the permission can be expressed as following: $permission^* : R \mapsto 2^{IP}$

$$permission(r_i) = \{(op, dcac, t_i) \mid \exists[(r_i, op, dcac, t) \in EPA] \wedge t_i \in M(t)\}$$

$$permission^*(r_i) = \{(op, dcac, t_i) \mid (\exists r \prec r_i)[(r_i, op, dcac, t) \in EPA] \wedge t_i \in M(t)\}$$

The secure workflow model is based on the roles. The explicit and implicit authority management can be expressed by the graphics as shown:

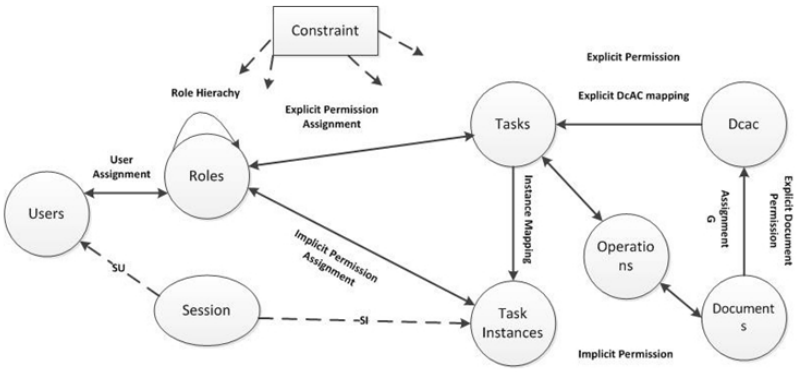

Figure.5: The secure workflow model which is based on the roles and the explicit, implicit authority management

4.3 The Analysis of the Safety and the Characteristics

(1) We discuss the authority relation between the roles and the tasks. And we also discuss the relation among the task instances, the documents, the tasks and the roles.

(2)We provide fine-grained access control. The task which is defined in the model is the smallest distinguished unit in the logic. We adopt the DcAC components and manage the document and the operation which are related to task instance. These measures improve the function of the authority management in the system greatly.

(3)It puts the concept of UA, EP, IP and IPA. They are responsible for the management and the access operation that the control roles to the object (the task, the data).

(4)It supports the two famous security principles.
①The principle of the least privilege. The user can obtain the related permission to execute the task access document according to activate the role. When the task execution document access is completed, the user must release the permission that it has obtained.
②The principle of the separation of duties. In the model, we distribute appropriate roles to the different tasks. It can achieve by selecting the appropriate user. During the modeling phase, it can only achieve the static separation of duties. For the dynamic separation for duties, it needs the WMS provide the corresponding historical components to achieve.

CONCLUSION

The computer technology and workflow technology have been applied to the office and enterprise widely. Workflow management system (WFMS) is facing more and more security problems to be solved. How to ensure the security of WFMS, protect the WFMS system and the security sensitive data have become a research focus in many research institutions.

This model uses the workflow based on the role as the background, and the workflow separates from the control level. We regard the workflow as a multilayer architecture to analyze the authorization of each level. In this model, the workflow model is divided into workflow layer, control layer and data layer. In the multi-state model, workflow layer and data layer is authorized through the detection of the events which are created in the control flow layer. At the same time, we design a secure workflow model based on the role and explicit, implicit authorization management of the combination between the workflow and RBAC96. Firstly, we state the model and put forward the concept of DcAC. It is used to manage and operate the documents which are related to the tasks. Secondly, we analyze the authorization relationship of the model and define the four concepts: EP, MEPA, IP and IPA. Then, we show the model by using the formal description and the graphical. The novelty of the model is that we put forward

the concepts of DcAC, UA, EP, EPA and IPA. It makes the workflow have some characteristics of the centralized authorized management, the neutral policy and the high security granularity. It also supports the principle of least privilege and the separation of duties.

REFERENCES

[1] LUO Haibin, FAN Yushun, WU Cheng. *Journal of software*, **2000**, 11(7): 899-907
[2] Fan yu-shun. Workflow management technology [M].Beijing, Qinghua University press **2001**
[3] FAN Yu-shun, WU Cheng. *Computer Integrated Manufacturing Systems*, **2000**, 6(1): 1-7
[4]Reinhardt A Botha, Jan H P ElofF. *IBM Systems Journal*. **2001**, 40(3), pp: 666-682
[5]Hollingworth D. Workflow Security Considerations-White Paper. The Workflow Management Coalition Specification, **1998**
[6]B.W. Lampson. Protection. In 5th Princeton symposium on Information Science and Systems, **1971**, pp: 437-443
[7]G_ S. Graham, P. J. Denning. Protection: Principles and Practice. In AFIPS Spring Joint Computer Conference, **1972**,pp: 417-429
[8]D. E. Bell, L. J. LaPadula. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, **1973**
[9]D. E. Denning. A Lattice *Communication of the ACM*, **1976**,: 236-243
[10]Thomas RK, Sandhu RS. Task-Based authentication controls (TABC): a family of models for active and enterprise-oriented authentication management. Proceedings of the 11th IFIPWG11.3 Workshop on Database Security. **1997**, pp: 165-172
[11]Sandhu RS, et al. *IEEE Computer* [J],**1996**, 29(2), pp: 38-47.
[12]J Wainer, P Barthelmess, A Kumar. *International Journal of Cooperative Information Systems*, **2003**,Vol. 12,No. 4,pp: 455-485
[13]David F. Ferraiolo,D. Richard Kuhn. Role-Based Access Controls.15th National Computer Security Conference. Baltimore, Oct 13-16,**1992**. pp: 554 – 563
[14]Bertino E, Ferrari E, Atluri V. *ACM Transactions on Information and System Security*. **1999**,2 (1), pp: 65-104.
[15]Reinhardt A Botha, Jan H P Eloff. *IBM Systems Journal*. **2001**, 40(3),pp:666-682
[16]Ferber, Jacques. Multi-Agent Systems An Introduction to Distributed Artificial Intelligence. Addison Wesley Iberoamericana, S. A. **1995**
[17]A. Cichocki and M. Rusinkiewicz. Migrating workflows. Advances in WorkflowManagement Systems and Interoperability, **1997**, pp: 311-326,
[18]Andrzej Cichocki,Marek Rusinkiewicz. Providing Transactional Properties for Migrating Workflows. Mobile Networks and Applications, **2004**, 9(5),pp: 473-480
[19]Wu Xiuguo, Zeng Guangzhou, *Expert systems with applications*, **2010**, vol(12), pp:8027-8035.
[20]Wu Xiuguo, Jiang Tongtong. Matchmaking of goals in intelligent agents based on description logics(DLs),in Proceeding- International Conference on Intelligent Computation Technology and Automation, **ICICTA2008**, pp: 806-810.
[21]Wu Xiuguo, Zeng Guangzhou, Gong Ping Yang. A Novel Approach for Describing Goals with DLs in Intelligent Agents. 4th International Conference on Natural Computation **ICNC2008**, pp: 226-230.
[22]Liu F, Zeng G *Expert Systems with Applications*. **2009**, 36(3), pp: 6995-7001
[23]Wang Rui, Zeng Guangzheu, *Journal of Central South University of Technology*, 201017(2):357-362
[24] WANG Hong , ZENG Guang Zhou. *Chinese Journal of Computers*,,**2001**,24 (4): 442-446