Advanced Materials Research Vols. 108-111 (2010) pp 426-435
© (2010) Trans Tech Publications, Switzerland
doi:10.4028/www.scientific.net/AMR.108-111.426

A CSCW-Enabling Integrated Access Control Model and its Application

Zhiyong Zhang[a], Tao Huang[b], Qingtao Wu[c] and Jiexin Pu[d]

Electronics Information Engineering College, Henan University of Science and Technology,
Luoyang, Henan 471003, P. R. of China

[a]zhangzy@mail.haust.edu.cn, [b]taohuang66@sohu.com,
[c]wqt8921@126.com, [d]pjx@mail.haust.edu.cn

Keywords: Computer Supported Cooperative Work; Access Control; Authorization; Formalism; Visual Modeling

Abstract. Nowadays open and distributed Computer Supported Cooperative Work (CSCW) systems are faced with security challenges due to large numbers of cooperative users, and a mass of valued data resources need to be protected against unauthorized usage, disseminations and share. To this end, role-based collaboration framework and access control approaches have been a focus in recent years, but there lack of a holistic and comprehensive model and visual modeling. We proposed and formalized a CSCW-enabling access control model integrating generic centralized authorization and distributed authority delegation, called IACM (Integrated Access Control Model) for CSCW, based on the cooperative roles and their owned activities. And then, the visual modeling was represented with static and dynamic characteristics, with a goal to narrow the gap of the formalized model and application level. Finally, an application in the collaboration system for equipments manufacture designing was implemented to improve security of the role-based centralized authorization management by using the authorization constraint rules, and to enhance the collaborative capability based on the user-side delegation mechanism, effectively guaranteeing CSCW system security and authorization management efficiency.

1. Introduction

The goal of CSCW system is realizing cooperative work and resource sharing among users on the heterogeneous distributed network platform, and access control ensures efficient and secure collaboration and resource sharing. In decades, the fruitful researches of CSCW access control have primarily concentrated on centralized authorization based on policy-neutral RBAC models and mechanisms. However, with the emerging large numbers of users and data objects, traditional authorization approaches are not suitable for the distributed CSCW environment, and centralized sever also would not endure burdensome authorization managements.

Recent years, the emerging delegation authority solves the above mentioned questions, and there are several related models and applications. Some issues and methods of role-based collaboration were addressed, such as role assignment and migration, role coordination, role collision and so on [1]. Anand Tripathi realized a role model and domain policy that meets dynamic security, but a formal model was not given [2]. A role-based access control model for CSCW was formally defined, and it focused on basic component and general authorization rules, not dealing with the needful delegation mechanism [3]. We proposed multi-agent based access control for role collaborations, including formalized model, secure protocol and architecture, and the scheme improve the CSCW system security and delegation authorization capability [4, 5, 6]. But, to date there lacks a holistic access control approach integrating general centralized authorization management with user-centric delegation mechanism.

The paper proposed a systematic CSCW-enabling access control model integrating centralized authorization and distributed authority delegation, and represented visual modeling and its application. The rest paper is organized as follows. Section 2 introduces the related works on access control models for CSCW. And then, Section 3 begins with the formalism of basic model components, as well as defines the temporal properties and several constraint rules. Section 4 and Section 5 addresses visual modeling and an application for CSCW system, respectively. The final section gives conclusions and future research.

2. Related Works

First, in recent years some role-based collaboration approaches have been already proposed, and Giacomo Cabri evaluates these approaches, presenting their main characteristics and comparing them each other. Moreover, he also proposed an interaction infrastructure, called Rolesystem, and this system allows agents to assume roles and interact accordingly in large-scale distributed web environments [7]. Moreover, as a role-based developing framework, BRAIN (Behavioral Roles for Agent INteractions) Giacomo Cabri proposed aims to cover the agent-based application development process at different phases [8]. Haibin Zhu's research aims to role-based collaboration in CSCW environment. Some issues and methods of role-based collaboration through practical applications were represented, such as role assignment and migration [9], role coordination, role collision [10, 11] and so on. Bo Lang provided a method to build a flexible security mechanism that separated the access control policy from the access control decision function by using the concept of meta-policy [12]. The flexible security mechanism can support multiple security policies dynamically.

Nowadays Multi-Agent System (MAS) is a hot topic in distributed artificial intelligent applications. As an important function of MAS, multi-agent collaboration research has focused on role-based methods that are very useful in building collaborative systems and resolving confliction in recent years [13]. The development of agent-based system must take into account interaction and collaboration, carefully modeling and engineering them, and roles represent a good concept that can help designers and developers deal with these questions [14]. Besides, in some applications of MAS, researchers and developers pay more attentions to multi-agent collaboration architecture and how to realize dynamic schedule, avoid collision, harmonize each other and cooperative work, and assure higher efficiency, security and stability of MAS. Andrea Omicmi introduced a role-based multi-agent cooperation model, architecture and related functions, but it lacked of model formalism [15].

Summarily speaking, these above mentioned related works do not involves generic holistic collaboration access control model and application, and the paper's goal is to solve the issue.

3 Formalized Integrated Access Control Model for CSCW

3.1 Basic Components

In order to solve the authorization management issue in a CSCW system with large numbers of users, and to improve cooperative authority' transfer and sharing, a novel CSCW-enabling integrated access control model, called IACM for CSCW, was proposed based on cooperative role and collaboration activities. The model embraces the two aspects of the generic authorization and acquired authority delegation, with typical features of centralization and distribution. IACM for CSCW is primarily composed of several basic components, such as cooperative user, cooperative role, permission, activity, task, session and constraint, as shown by Fig.1.

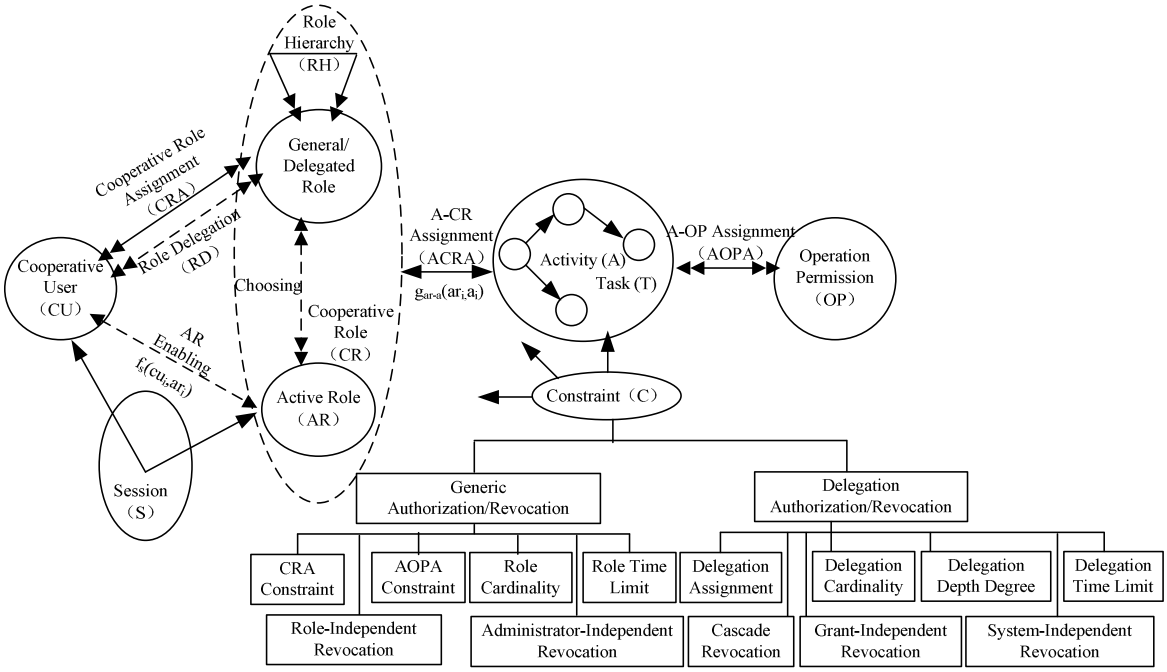

Fig.1 IACM for CSCW

3.2 Main Formalism

There is a group of key components in IACM for CSCW: CU, CR, AR, T, A, OP, C, are defined as sets of cooperative user, cooperative role, active role, task, activity, operation permission and constraint, respectively. By using the classical set theory and first-order logic, IACM is primarily formalized as follows.

Definition 1 (Cooperative User, CU): CU is an active Cooperative Entity (CE) that accomplishes an object collaboration task. It could be a generic user or agent, and CU is further subdivided into two subsets as the task Sponsor and Cooperator.

$$CU=\{cu|cu\in \text{Sponsor} \vee cu\in \text{Cooperator},\ cu\in \text{User} \vee cu\in \text{agent}\}$$

Definition 2 (Cooperative Role, CR): it denotes an abstract kind of cooperative users with an identical task, and *ar* (Active Role) is one and only one effective role for *cu* in a session, where *cu* could accomplish an activity or access to data resources.

$$CR\in 2^{CU}(cu\in CU,\ ar\in CR(cu))$$

Definition 3 (Task & Activity): CU's collaborative goal is specified as a task, and the every step is called activity, which is an essential unit of the task, and has dynamic and atom characteristic. The activity is formalized as a set of *op* (Operation Permission).

$$\forall t\ (t\in T)\ t = \{a_1, a_2, \ldots, a_n \mid a_i\in A\}$$
$$\forall a\ (a\in A)\ a = \{op_1,op_2\ldots op_n \mid op_j\in OP\}$$

Definition 4 (Set Relationship): there exist the important relationships in IACM for CSCW as follows,

$CRA \subseteq CU \times CR$: it is a multiple-to-multiple relationship between CU and CR.

$ARE \subseteq CU \times AR$: Active Role Enabling is a one-to-one bijective function $f_s(cu_i, ar_i)$.

$ACRA \subseteq A \times CR$: there exists a one-to-one relationship, that is a bijective function $g_{ar-a}(ar_i, a_i)$.

$AOPA \subseteq A \times OP$: a multiple-to-multiple relationship indicates an assignment procedure of the operation permissions, such as read, write, execute, and download.

$RH \subseteq CR \times CR$: Role hierarchy is a partial order set for CR.

Definition 5 (Cooperative Role Assignment, CRA): the authorization is a triple-tuple (cu, cr, Constraints), and it denotes *cu* would acquire *cr* when the assignment condition is consistent with constraints rules including the temporal limits.

Definition 6 (Role Delegation, RD): the delegation authorization is formalized as a six-tuple (cu_1, cu_2, DRG, DTL, Constraints), where cu_1 is a delegator, cu_2 is a delegtee, DRG (Delegated Role Group) is a set of assigned roles, DTL (Delegation Time Limit) is the limitation of periodic or piecewise delegation times. The relation's semantic is the user cu_1 could delegate DRG to another cooperative user, thereby cu_2 would acquire the whole explicit and implicit operation permissions in prerequisite conditions of DTL and constraints.

Property 1 (Cascade Delegation Revocation): When an original user revokes delegation or the system time exceeds DTL, the whole roles and permissions of DRG will be revoked in the multi-step delegation chain.

Property 2 (Grant-Independent Revocation): Every delegator in the delegation path could revoke delegated roles/permissions, besides the original delegator has the right to revocation.

Property 3 (System-Independent Revocation): If the system time exceeds to DTL of DRG or other requisite conditions change, CSCW system would automatically revoke the authority including all explicit and implicit general authorization and delegation, without the consideration of the authority delegation system.

3.3 Temporal Properties for Cooperative Role and Activity

The following definitions denote the temporal properties for CR and its corresponding activity.

Definition 7 (Role Time Limit, RTL): IACM for CSCW has the property of time limitation, DTL=$\{x \mid x=[\tau_{bi}, \tau_{ei}](i=1,2\ldots n)\}$, where τ_{bi} is beginning-time , and τ_{ei} is end-time.

Definition 8 (States Set): The states set of role S={init, invoke, sleep, expire}, *init* is a beginning-state, *invoke* is an active-state, *sleep* is a sleepy-state and *expire* is a exiting-state. Here CR's expire-status is not equal to the role revocation. If expired, the role could be set on RTL/ DTL again, or be revoked.

Definition 9 (State Transitions): Let *ST* be system time, State *s* meets the following transition modes: $\forall i(i\in N)\ ST\notin[\tau_{bi}, \tau_{ei}] \wedge ST<\tau_{b1} \rightarrow S=\mathit{init}$, $\exists i\ (i\in N)ST\in[\tau_{bi}, \tau_{ei}] \rightarrow S=\mathit{invoke}$, $\forall i(i\in N)ST\notin[\tau_{bi}, \tau_{ei}] \wedge (ST>\tau_{b1}) \wedge (ST<\tau_{en}) \rightarrow S=\mathit{sleep}$, $\forall i(i\in N)ST\notin[\tau_{bi}, \tau_{ei}] \wedge ST>\tau_{en} \rightarrow S=\mathit{expire}$.

Property 4 (Temporal Order for Activity): The relation of activities is synchronization or concurrent. Between every two activities exits steady time order that meet partial order relation, denoted by "□".

$$\forall t, a_i, a_j\ (t\in T, a_i, a_j\in A)(a_i\in t \wedge a_j\in t \rightarrow a_i \square a_j)$$

$$\forall t, a_i, a_j, a_k(t\in T, a_i, a_j, a_k\in A)(a_i \square a_j \wedge a_j \square a_k \rightarrow a_i \square a_k)$$

Property 5 (Running Order for CR): CR is executed in serious or concurrently, and is partial order, denoted by " $>_{RO}$".

$$\forall t, cr_i, cr_j, cr_k(t\in T, cr_i, cr_j, cr_k\in t)(cr_i >_{RO} cr_j \wedge cr_j >_{RO} cr_k \rightarrow cr_i >_{RO} cr_k)$$

Property 6 (Temporal Order Consistency for Activity-CR): Activity and CR is consistent in time order owing to their one-to-one mapping relation. Predication "Related(cr_i, a_j)" denotes cr_i is related to a_j.

$$\forall t, a_i, a_j, r_i, r_j(a_i, a_j\in t)\ (\text{Related } (cr_i, a_i) \wedge \text{ Related } (cr_j,a_j)\ \wedge\ a_i \square a_j \leftrightarrow cr_i >_{RO} cr_j)$$

3.4 Constraint Rules for Cooperative Role and Operation Permission

IACM for CSCW strengthens cooperative role/operation permission assignment managements, preventing malicious user from deliberately or involuntarily acquiring illegal privileges, as well as improving system security and controllability. Several essential rules, including CR/OP non-collision constraint and role cardinality, were defined as follows.

Definition 10 (Operation Permission Collision): Two operation permissions op_i and op_j are collision capabilities, if they are not assigned to a user cu_k at the same time, as denoted by Coll_OP(op_i, op_j, cu_k).

Definition 11 (Cooperative Role Collision): Two cooperative roles cr_i and cr_j are collision roles, if they are not assigned to a user cu_k or are activated at the same time, as formalized by Coll_CR(cr_i, cr_j, cu_k).

Constraint Rule 1 (Non-Collision Constraints): Any two operation permissions or cooperative roles have not assignment collisions in CR and OP sets.

$$\forall\ op_i, op_j\ (op_i \in OP, op_j \in OP, cu_k \in CU)\ \mathrm{Coll\_OP}(opi, op_j, cu_k)=\mathrm{False}$$

$$\forall\ cr_i, cr_j\ (cr_i \in CR, cr_j \in CR, cu_k \in CU)\ \mathrm{Coll\_CR}(cr_i, cr_j, cu_k)=\mathrm{False}$$

Definition 12 (Role Cardinality): Role cardinality is the maximal number of users who could acquire a certain role. Thus, each user's the role number in CR does not exceed its pre-defined cardinality that is a natural number commonly.

4 IACM for CSCW Visual Modeling

4.1 Static Visual Modeling

Object-oriented method including object-oriented analysis and designing is the approach of designing system and developing software using the following concepts, such as object, class, inheritance, encapsulation, aggregation, message transfer, and polymorphism [6]. In distributed computing environment, IACM for CSCW resolves the issue of authorization complexity owing to centralized administration. There needs the visual modeling for CSCW system implementations by the object-oriented thinking and UML, which supports object-oriented analysis and designing, thus shortening the gap of abstract model and application implementations, together with benefiting the designing and development applications based on the proposed model.

With regard to static modeling of IACM for CSCW, use case diagram, entity class and class relationship diagram are mainly represented. System functions are introduced from user's perspective by using use case diagram, and users are basically subcategorized into four kinds, which fulfill different functions respectively. System Administrator manages the assignment of users, regular cooperative roles and privileges. Security Officer takes charge of regular authorization constraints and delegation constraints, thus carrying out the constraints of role, permission and session, System Auditor mainly tracks operations of system administrators' authorizations, and audit delegation processes and data access to cooperative works resources. Cooperative Entity, i.e. CU, can create and close activity sessions, delegate DRG to others and access to object data. The functional use case is illustrated as Fig 2.

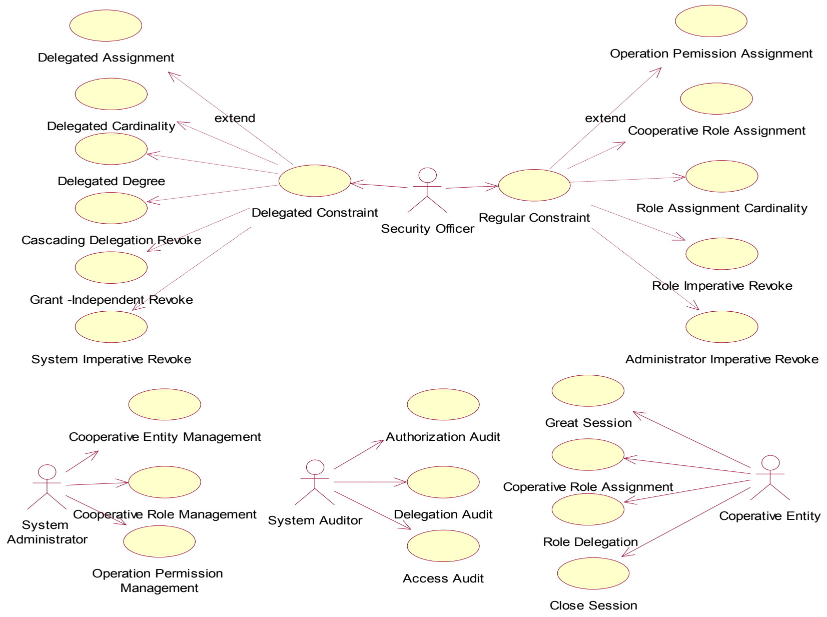

Fig.2 Use Case Diagram

Some important entity classes, which refer to attributes and methods, and class relationships can be used to present IACM for CSCW's static characters. These relationships mainly include generalization, aggregation and association. Role class is generalized into two subclasses: regular role and DRG, which inherit the public attributes and methods of parent-class, as well as possessing private attributes and methods respectively. Constraint class is also generalized into Role Assignment Constraint, Permission Assignment Constraint, Role Temporal Limitation, Revocation, as well as a series of Role Delegation Constraints. These constraints have effects on the constraint rules control over role and permission assignments and delegations, respectively. In the association relationship, the cardinality characteristic between classes should be represented, such as many-to-many associations between cooperative entity and role, cooperative entity and DRG, task and permission, as well as one-to-one associations among cooperative entity-session-activity, together with between role and activity. Besides, the relationship between task and activity class is a special aggregation named as composition, as shown by Fig.3.

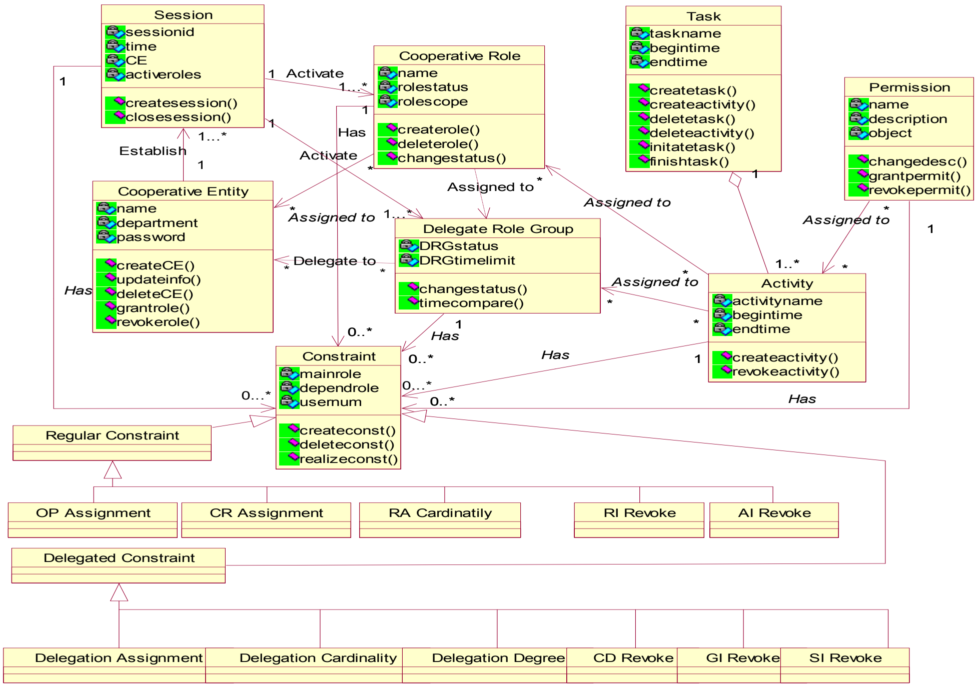

Fig.3 Classes Relationship Diagram

4.2 Dynamic Visual Modeling

With respect to dynamic modeling, interaction diagram and object behavior diagram are shown by Fig 4 and Fig.5. All dynamic characters are not described due to the length limitation of the paper, followed by regular role assignment and role delegation sequence diagram (a kind of interaction diagram). Here, the procedure of the system administrator's assignment for a regular user to the related cooperative role is illustrated by Fig.4, and the cooperative role delegation between users is depicted by Fig.5. In the above mentioned two procedures, related constraints rules and mechanisms are effectively activated, together with some accomplished audit operations.

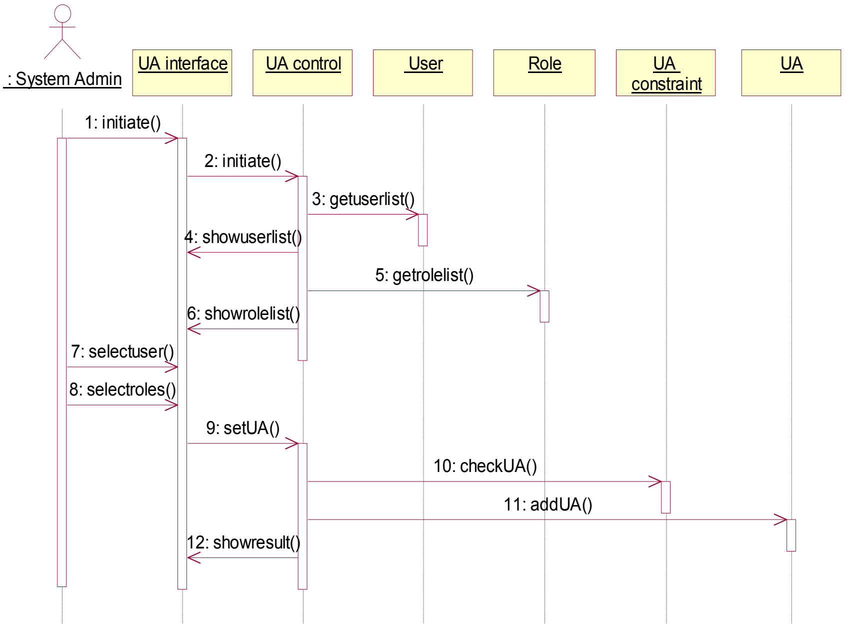

Fig.4 Sequence Diagram of Cooperative Role-User Assignment Authorization

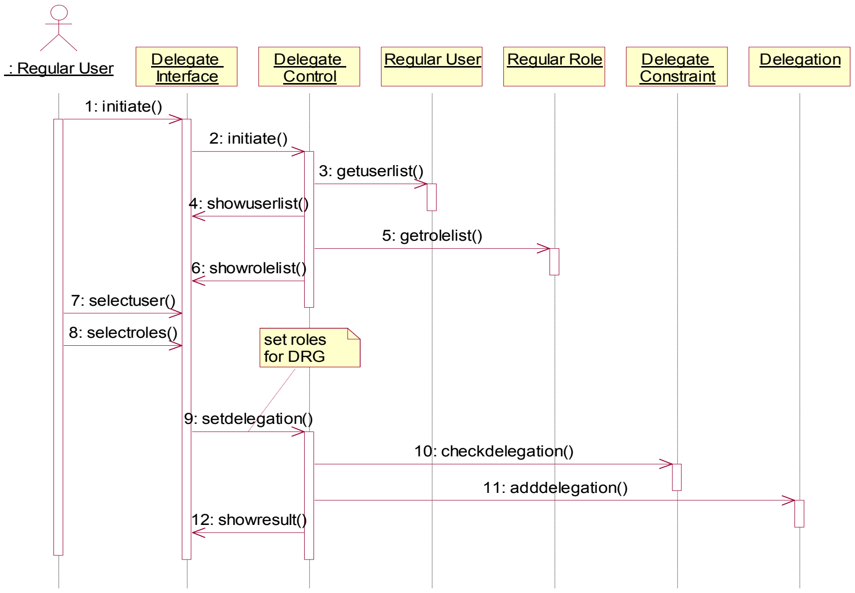

Fig.5 Sequence Diagram of Cooperative Role Delegation Authorization

5. IACM for CSCW Application in Equipment Manufactures Collaboration Designing

In the security subsystem of the collaboration application named as EMCDS (Equipments Manufacture Collaboration Designing System), IACM for CSCW was employed, as shown by Fig.6. The architecture is composed of authorization, authentication, access decision and control. The authorization managements are mainly composed of centralized authorizations, distributed delegations, management databases and constraint rules database. The users of EMCDS are also subdivided into a cooperative user, system administrator, security officer and auditor by using security principle "Separation of Duty". In centralized authorization, the system administrator could assign a certain cooperative role to a user in combination with general authorization constraints in the above mentioned constraint rules database. The security officer administrates the rule database according to application-level security policies, and auditor should answer for some audit operations, that is recording and tracking authorization process, especially for distributed delegation authorizations.

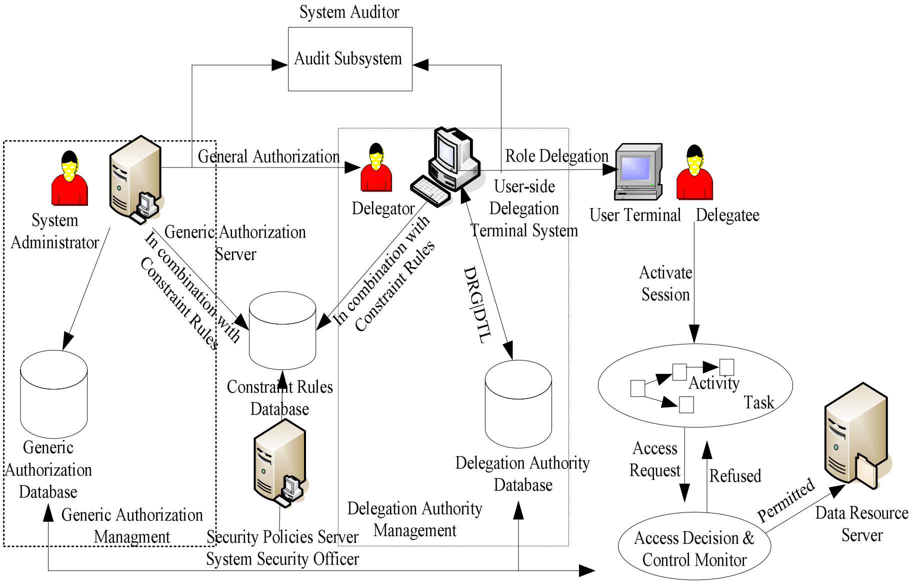
System Auditor
Audit Subsystem
General Authorization
Role Delegation
System Administrator
Generic Authorization Server
Delegator
User-side Delegation Terminal System
User Terminal
Delegatee
In combination with Constraint Rules
In combination with Constraint Rules
DRGDTL
Activate Session
Activity
Task
Constraint Rules Database
Generic Authorization Database
Delegation Authority Database
Access Request
Refused
Permitted
Data Resource Server
Generic Authorization Managment
Security Policies Server
System Security Officer
Delegation Authority Management
Access Decision & Control Monitor

Fig.6 Access Control Framework of EMCDS

Besides, the delegation authorization of EMCDS is an open and distributed architecture, and a user discretionarily delegates his/her cooperative capability instead of the centralized administration. Here, a delegation terminal system is used for implementing the user's delegation of role(s)/permission(s) after receiving for other cooperators' requests. In Fig.6, a delegtor could choose his object delegtee, DRG, DTL through the user-side delegation terminal system, and the whole delegation process must be consistent with delegation constraint rules. If no consistent, the delegation would be refused. After accepting DRG and requisite access permission(s), delegatee could share data resources with the delegator. Note that Access Decision & Control Monitor makes decision on an access request based on the general authorization and delegation servers.

6. Conclusions

IACM for CSCW is a general systematic CSCW access control reference model supporting cooperative role assignment, delegation, constraints rules on the basis of cooperation activities and tasks. Our visual modeling presented static and dynamic characteristics regarding to general authorization and delegation. The future works focus on temporal constraints' implicit and explicit expressions and conflicts resolve, so that enrich the integrated theoretical model and its application scenarios.

Acknowledgement

The authors want to thank anonymous reviewers for their valuable comments and suggestions. The work was sponsored by National Natural Science Foundation of China Grant No.60803150, Henan Province Key Technologies R & D Program Grant No.092102210295, and Henan University of Science & Technology Young Scholar Fund Grant No.2008QN010.

References

[1] H. Zhu: Some issues of Role-Based Collaboration. In: Proc. of IEEE Canadian Conference on Electrical and Computer Engineering, p. 687-690, Montreal, Canada, May (2003).

[2] A. R. Tripathi, T. Ahmed and R. Kumar: Specification of Secure Distributed Collaboration System. In: Proc. of the sixth International Symposium on Autonomous Decentralized Systems, p. 149- 156, Pisa, Italy, Apr (2003).

[3] C. Li, Y. Zhan and L. Xie: A Role-Based Access Control Model for CSCW Systems. Journal of Software, Vol.11, No.7, p.931-937 (2000).

[4] Z. Zhang, J. Pu and S. Zhang: Dynamic Capability Delegation Model for MAS, Architecture and Protocols in CSCW Environment. In: Proc. of the 10th International Conference on CSCW in Design, p. 602-607, Nanjing, China, May (2006).

[5] Z. Zhang, J. Pu: Collaboration Access Control Model for MAS Based on Role and Agent Cooperative Scenarios. In: Proc. of 2006 IEEE International Conference on Mechatronics and Automation, p. 825-830, Luoyang, China, June (2006).

[6] Z. Zhang, H. Zhang and J. Pu: Delegation Model for CSCW Based on RBAC Policy and Visual Modeling. In: Proc. of the 11th Joint International Computer Conference, p.126-130, World Scientific Press Company, Chongqing, China, Nov (2005).

[7] C. Giacomo, L. Letizia and Z. Franco: Implementing Role-based Interactions for Internet Agents. In: Proc. of 2003 International Symposium on Applications and the Internet, p.380, Orlando, Florida, USA, Jan (2003).

[8] C. Giacomo, L. Letizia and Z. Franco: Role-based Approaches for Engineering Interactions in Large-scale Multi-Agent Systems. In: Software Engineering for Multi-Agent Systems II, Pereira

de Lucena, Garcia, Romanovsky, Castro, and Alencar editors, Lecture Notes in Computer Science Vol. 2940, p.243-263, Apr (2004).

[9] H. Zhu and P. Seguin: The Role Transition Mechanisms in Role-Based Collaborative Systems. In: Proc. of IEEE Canada Conference on Electrical and Computer Engineering, Saskatoon, Canada, p.1305-1308, May (2005).

[10] H. Zhu: A Role-Based Conflict Resolution Method in a Collaborative System. In: Proc. of IEEE International Conference on Systems, Man, and Cybernetics, Vol. 5, p. 4135-4140, Washington D C, USA, Oct, 2003.

[11] H. Zhu: Conflict Resolution with Roles in a Collaborative System. International Journal of Intelligent Control and Systems, Vol. 10, No.1, p.11-20 (2005).

[12] B. Lang ,Y. Lu, X. Zhang and W. Li: A flexible access control mechanism supporting large scale distributed collaboration. In: Proc. of the 8th International Conference on Computer Supported Cooperative Work in Design,Vol.1, p.500- 504, May (2004).

[13] H. Zhu: Role Mechanisms in Collaborative Systems. International Journal of Production Research, Vol. 44, No. 1, p.181-193, Jan (2006).

[14] C. Giacomo, F. Luca and L. Letizia: Agent Role-based Collaboration and Coordination: a Survey about Existing Approaches. In: Proc. of the 2004 IEEE Systems, Man and Cybernetics Conference, Vol.6, p 5473-5478, Hague, Netherlands, Oct (2004).

[15] A. Omicmi, A. Ricci and M. Viroli: RBAC for Organization and Security in an Agent Coordination Infrastructure", Electronic Notes in Theoretical Computer Science, Vol.128, p. 65-85 (2005).