Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080365

OB4LAC: An Organization-based Access Control Model for E-government System

You Peng[1,*], *Yan Song*[1], *Hang Ju* [1] *and YanZhang Wang*[2]

[1] Department of Management and Economics, Harbin Engineering University, Harbin 150001, China
[2] Department of Management, Dalian University of Technology, Dalian, 116024, China

Received: 6 Jul. 2013, Revised: 10 Nov. 2013, Accepted: 11 Nov. 2013
Published online: 1 May. 2014

Abstract: Following the emergency of multi-level, complex and distributed information systems, the traditional RBAC model becomes more and more weak and incompetent. Currently, the research of RBAC model mainly focused on building a suitable role hierarchy, although played a certain effect it still have many problems. Through the research aiming at organizations and their characters, we believe that the reasons that cause the present problems are due to the conflict in working patterns between the RBAC model and the physical world. Thus, we propose a new access control method-Organization Based Access Control Method and the specific model-OB4LAC model. This article analyzes the constituent members, formal specification, sub-models UPA, PORA, PERA and RRA of OB4LAC, and also gives the specific process in access operations and business collaboration among multi-organizations. Through the test in many complex E-government systems, OB4LAC model achieves good results.

Keywords: OB4LAC, Access Control, Authorization Management, Information Security

1 Introduction

Currently, the RBAC model is widely used in the authorization management of E-government systems for the reasons of which can effectively implement the logic separation of users and authorization, reduce the complexity of authorization management through the introduction of the conception of “Role”. RBAC model not only improves the discretionary and mandatory of traditional access control (DAC and MAC) models, but also provides solutions for solving access control problems in the distributed information systems. However, as the scale of the information system expands rapidly, RBAC model encounters many difficulties. In current complex systems, there can be hundreds of users and thousands of roles, and the number of application program or information objects are even more huge, but the work to manage these users, roles and system resources are responsible by the limited security administrators, which not only increase the workload of them, but also not suitable to the actual working pattern in authorization management. Therefore, how to improve the existing RBAC models and make them adaptable to the growing needs of the current information system are the focus research to the experts and scholars all over the world.

2 Related Works

Experts and scholars have done a great deal of works in the fields of improving RBAC model, and achieved many good effects. Sandhu proposed the RBAC96 model in 1996, which first used the conception of inheritance relationship among roles [1]. Then, he proposed ARBAC97 model and divided the conception of role to two types, general roles and management roles, and presented the management relations between them[2]. ARBAC02 model is based on the ARBAC97 model, it uses the conception of “Organization Structure” to improve it, but ARBAC02 model did not explain how to manage role hierarchy[3]. F. Cuppens proposed a new access control model Or-BAC model based on the association rules [4,5], which uses the method of role hierarchy relation to represent organizational structure, but the association rules could not represents the whole organizational structure. SEJONGOH proposed OS-RBAC model[6], which uses the organization

* Corresponding author e-mail: penggoto2008@sina.com

structure management model and role management model to improve the relationship between access management and organization structure, but it still did not discuss the problems in the organization structure management.

Thus, we can conclude that the current research still want to build a suitable role hierarchy for RBAC model, and base on it to achieve the goals of authorization management and access control, which would control the complexity of access control model in a certain degree, but it can't solve the inherent flaws of RBAC model. Through the actual development work in many E-government system, we believe that the main reasons caused those problems are due to the conflict in working pattern between the RBAC model and the physical world. It reflects in the following points:

1. RBAC model break the organization structure in the real world and ignore the effects of position, which is the basic node of the organization. Although the conception of role in the RBAC model covers the conception of position in a certain degree, but it is still more suitable to information systems since it always represent the collection of information operations; but the conception of position is the real component to a real organization. So we can see the conception of "Role" and "Position" is similar but not equal.

2. In RBAC model, the assignments among user-role-permission-system resource are responsible by the security administrators, but actually the assignments of users and authorization are responsible by the human resource department and the IT department. RBAC model break the actual working pattern of organizations in the physical world, which not only bring heavier workload to the security administrators, but also make the authorization management in disorder.

3. When a user assigned to different roles in different application programs wants to change his authorizations in RBAC model, the security administrator has to do much repeated work, as shown in Fig1.a. But the change frequency of authorization belonging to a position is much slower, so the "Position" would reduce the repeated authorized work greatly, as shown in Fig1.b.

4. RBAC model is more suitable for a single information system environment. When facing the authorization management among multi-organizations, it would usually adopt the method of "Role Mapping", but this method would expand the authorization of a role in some cases, as shown in Fig.2. The roles R_{a2}, R_{a3} in organization A and R_{b2}, R_{b1} in organization B establish the role mapping relations, which means R_{a2}, R_{b1} also have the authorization of R_{b2}, R_{a3}, then we find that R_{a2} can acquire the authorization of R_{a3} by the path: $R_{a2} \rightarrow R_{b2} \rightarrow R_{b1} \rightarrow R_{a3}$, that is to say, R_{a2} can acquire the authorization which should not authorize to it; this would make the authorization management of system out of control. From the viewpoint of system science, the authorization management among multi-organizations is based on the organizational behavior, and which only can be done by the organizations' communication and trust.

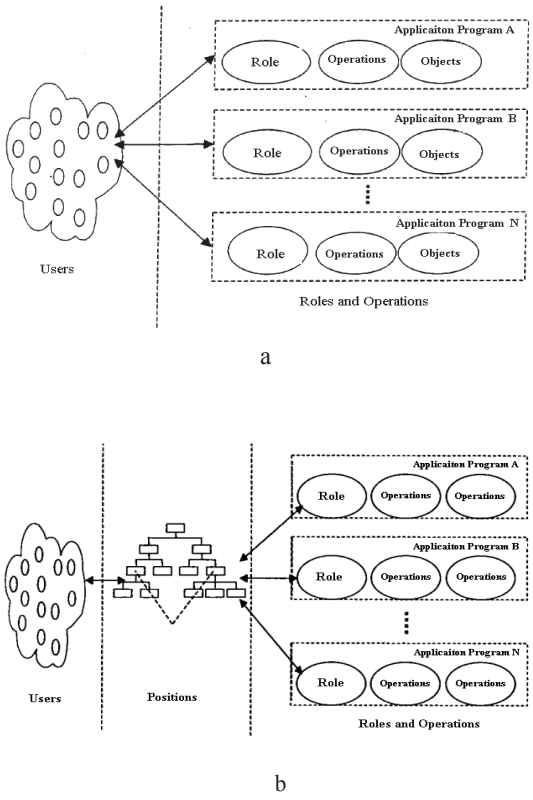

Fig. 1: The initial authorization system and modified authorization system in RBAC

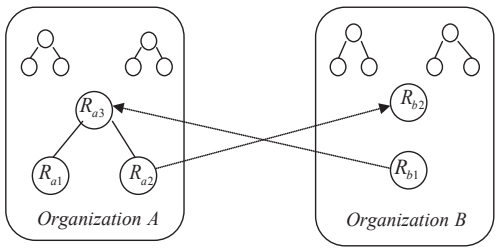

Fig. 2: Role Mapping in RBAC

Through the research about the complex E-government system in China, this paper proposed a new access control method - Organization Based Access Control Method and its specific model-OB4LAC (Organization Based 4 levels Access Control Model), try to use the viewpoint of organization management to solve the problems of authorization management in todays complex E-government system.

3 The Access Control Theory Based on Organizations

3.1 Organization, Organization Structure and Position

The conception of organization comes from the social division of labor, and it becomes more and more complex following with the improvement of science and increasing of social production. Along with the expansion of activities in modern society, organizations need complex cooperation to achieve the goals and become important and irreplaceable. The conception of organization structure represents the specific work and functions of the constituents within an organization, which not only determines the integrity of this organization, but also provides specific methods for coordination and communication. For example, government is a typical complex organization which composed by a certain purpose, it not only establishes the steady organization structure, but also build the mechanism of cooperation and communication among internal departments. The conception of position refers to the job, which is the basic execution unit of authorization in an organization; it is the node of an organization structure and the smallest unit to undertake the work of an organization. To a specific government, all responsibilities and authorization should be based on position, any user would have the corresponding responsibility and authorization when he is in the position and lost it when not.

3.2 The Access Control Theory Based On Organizations

Through the analysis of the conception of organization, organization structure and position, we can find that the current research for RBAC model ignore the importance of the organization characters in E-government system and still use the conception of role as the center in authorization management, which not only unsuitable to the actual working pattern of government in the physical world, but also has much conflict with the current management mechanism.

In this paper, we believe that the authorization management in E-government system should first consider the characters of organization about government, and thus the conception of position has its irreplaceable function. So, we propose a new access control theory based on organization, specifically, the authorization management in E-government system should adopt the viewpoint from the whole organization and understand the detail responsibility and authorization of each individual or department in the organization, to make sure that they would be in the best condition. When dealing with the cooperation and communication among multi-organizations, we regard it as the coordination of benefits and need to establish trust mechanism to achieve the purposes of access operations Essentially, the access control method based on organization use the perspective of system engineering; make the organization as the core of authorization management to solve the problems in RBAC model that discussed above.

4 OB4LAC- Organizations Based Four Levels Access Control Model

Based on the organization-based access control method, we propose a new access control model: Organization Based 4 levels Access Control Model - OB4LAC. Firstly, OB4LAC model improve the RBAC model through the approach of adding a layer of “position”, which expand the models structure from user - role - permission to user - position - role - permission. Secondly, it changes the core of authorization management from “Role” to “Position”, and through the viewpoint of organization management to solve the security problems of access operations and business cooperation among multi-organizations. OB4LAC model adopt the perspective of organization, and full play the responsibility and authorization of each departments in the organization, the assignments of user C position, role - permission are responsible by the human resource and IT department respectively, the security management department are only responsible for the assignment among position-role. So we can find that the OB4LAC model is suitable to the actual working pattern of government in the physical world, and each department of the organization can acquire the best condition. Fig.3. Show the detail relationship between the specific constituent members in the OB4LAC model.

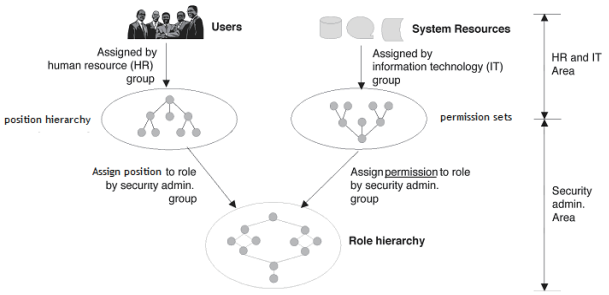

Fig. 3: The detail relationship between the specific constituent members in the OB4LAC model

Definition 1. the OB4LAC model can be represented as a six-tuple $(USR, POS, ROL, PER, SESS, TIM)$, here, USR represent the user set, POS represents the position set, ROL represents the role set, PER represents the permission set, $SESS$ represents the session set, TIM represent the time set.

Definition 2. USR represent the user set, $USR = (ORG, TEAM, INF)$, here, ORG represent the organization that the user is belonged to, $TEAM$ represent the dynamic team which is divided by the tasks or functions, and INF represent the information of this user.

Definition 3. POS represent the position set, and it is the standard execution unit in an organization, $POS = (ORG, TYPE, ATTR, INF)$. Here, ORG represent the organization that the position is belonged to, $TYPE$ represent the type of this position, $ATTR$ represent the attribute of this position, and INF represent the information of this position.

Definition 4. ROL represent the role set. Here, $ROL = \{rol_1, rol_2, ..., rol_n\}$, rol_i $(i \in \{1, 2, ..., n\})$, represent the No.i role and the number of total roles is n. The definition of role in OB4LAC model is the same as the RBAC model.

Definition 5. PER represent the permission set. Here, $PER = (NAME, BOL, BOC, RES)$. $NAME$ represent the name of permission, BOL represent the collection of information objects that this permission can handle, BOC represent the operation collection of this permission, and RES represent the information resource that this permission can handle.

Definition 6.

$UPA \subseteq usr \times pos$: user-position assignments;

$PORA \subseteq pos \times rol$: position-role assignments;

$PERA \subseteq rol \times per$: role-permission assignments;

$user : sess \rightarrow usr$: a function mapping a session to a single user;

$assigned\_usr - pos = \{pos | (usr, pos) \in UPA\}$: A function mapping a user to a detail position;

$usr : pos \rightarrow 2^{usr}$: a function mapping a position to a set of users belong to it;

$PH \subseteq pos \times pos$: position hierarchy;

$RH \subseteq rol \times rol$: role hierarchy,

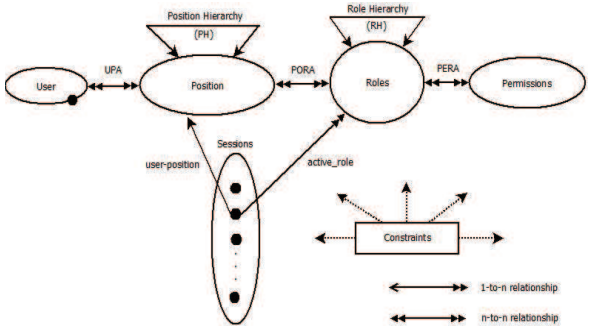

Fig. 4: Summary of OB4LAC model

4.1 UPA

UPA sub-model is used to manage the assignments among user - position. From the perspective of organization management, we divide the conception of "Position" into two types: specific position and general position, each type of position also have two attributes, which are real position and virtual position. Specific position represents an existing position in an organization, for example, a project manager or a business executive, etc; while general position is not an existing position but can acquire the corresponding authorization through the trust relationship among multi- organizations in the process of access control and business cooperation, such as an auditing officer, software engineer, and citizen etc. The position hierarchy in UPA sub-model is not on behalf of the authorization in the organization, but only means the level of position, so the high-level positions cannot inherit the authorization from the lower one, which is suitable to the actual working pattern of an organization in the physical world. In UPA sub-model, a user's authorization is only controlled by the definition of their position but not the level. Fig.5. shows a detail example for a position hierarchy structure in a government.

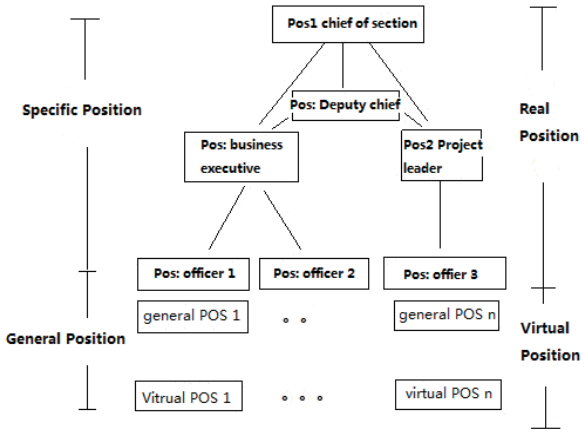

Fig. 5: A position hierarchy structure in a government

The assignments of the relationship among user - position in UPA sub-model are responsible by the human resource department, and the working pattern of this department is not the focus of our study so we do not discuss it here. UPA sub-model includes two management functions: *can_assign_user* and *can_revoke_user*, they are used to assign and revoke the relationship among user - position.

Definition 7. the management functions to assign and revoke the relationship among user - position:
$can\_assign\_user : Sess \times Usr \times Pos \rightarrow \{true, false\}$, if the function returns TRUE, then the user assign to the

position successfully in current session.
can_revoke_user : $Sess \times User \times Org \rightarrow \{true,\ false\}$, if the function returns TRUE, then the user revoke to the position successfully in current session.

4.2 PORA AND PERA

PORA and PERA sub-models are used to manage the assignments among position-role and role-permission. To improve the efficiency in authorization management, OB4LAC model use the same management method to the conception of "Role" as RBAC model, which means that the "Role" have the hierarchy and inherit relationship. One position does not have any authorization until the roles assigned to it. Fig.6. shows a specific PORA sub-model in an organization.

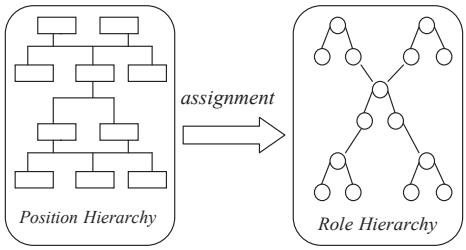

Fig. 6: A position hierarchy structure in a government

Definition 8. the management functions to assign and revoke the relationship among position C role:
can_assign_role : $Sess \times Pos \times Rol \rightarrow \{true, false\}$, if the function returns TRUE, then the role assign to the position successfully in current session.
can_revoke_role : $Sess \times Pos \times Rol \rightarrow \{true, false\}$, if the function returns TRUE, then the role revoke to the position successfully in current session.

Definition 9. the management functions to assign and revoke the relationship among role C permission:
can_assign_permission : $Sess \times Per \times Rol \rightarrow \{true, false\}$, if the function returns TRUE, then the assign to the successfully in current session
can_revoke_permission : $Sess \times Per \times Rol \rightarrow \{true, false\}$, if the function returns TRUE, then the revoke to the successfully in current session

4.3 RRA

RRA sub-model is used to manage the role hierarchy, and it uses the function *can_modify_R* to deal with it.

Definition 10. the management functions in RRA sub-model.
$can\_modify\_R : S \times 2^{Rol} \rightarrow \{true, false\}$, if the function returns TRUE, then the user set $User(S)$ has the permission to modify the assignment in role set *rset*.

From the actual working pattern of government in the physical world, we can find that a senior position does not cover all the authorization belong to a junior one, in other words, the junior one can also has some private authorities. Thus, we divide the inheritance relationship of RRA sub-model into two types, which are "all connected inheritance relationship" ("-") and "none connected inheritance relationship" ("..."), and combining the members' state machines to solve the private authorities of junior position.

Table 1: The members' state machines in RRA sub-model

Predicate	Meaning
$pos\_assigned(u, pos, r, t)$	(u, pos) is assigned to role r at time t
$can\_be\_acquire(per, r, t)$	role r can acquire the permission per at time t
$can\_not\_acquire(per, r, t)$	role r cannot acquire the permission per at time t
$can\_activate(pos, r, t)$	The position pos can active role r at time t, but not yet
$can\_not\_activate(pos, r, t)$	The position pos cannot active role r at time t
$activate(pos, r, t)$	The position pos active role r at time t successfully
$can\_acquire(u, pos, r, per, t)$	(u, pos) can acquire the permission per of role r at time t

The all connected inheritance relationship in RRA sub-model represents that the senior role inherits all authorities of the connected junior roles directly. That means if there have the roles $R_x, R_y, R_x \geq R_y$, R_x can inherit all authorities of R_y.

$$\forall per,\ (R_x \geq R_y) \wedge can\_be\_acquire(per, R_y, t) \rightarrow can\_be\_acquire(per, R_x, t)$$

The None connected inheritance relationship in RRA sub-model represents that the senior role cannot inherit any authorization of the connected junior roles (rule a), but the senior position that assigned to the senior role can active this junior role (rule b), and only when the senior position active the junior role successfully it can acquire all authorities belong to this junior role (rule c).

a. $\forall per,\ \exists(R_x \geq R_y) \wedge can\_be\_acquire(per, R_y, t) \rightarrow can\_not\_acquire(per, R_x, t)$

b. $\forall u,\ \forall pos,\ \exists(R_x \geq R_y) \wedge pos\_assigned(u, pos, R_x, t) \rightarrow can\_activate(pos, R_y, t)$

c. $\forall u,\ \forall pos,\ \forall per,\ pos\_assigned(u, pos, R_x, t) \wedge activate(pos, R_y, t) \rightarrow can\_acquire(u, pos, R_y, per, t)$

Through the approaches of "all connected inheritance relationship" and "none connected inheritance

relationship", the junior position can have the private authorities on the one hand, but on the other hand it allows the senior position to acquire these authorities through the method of activation. This method is suitable to the actual working pattern of government, for example in Fig.7, the junior position pos_2 have the private authorities that the senior position pos_1 cannot acquire, only when the position pos_1 active the junior role R_b successfully it can acquire these authorities, and the system also can regulate a series of active constraints to manage these private authorities.

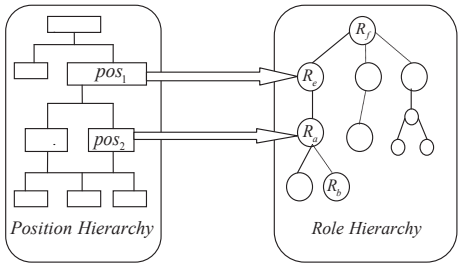

Fig. 7: The authorization management in RRA sub-models

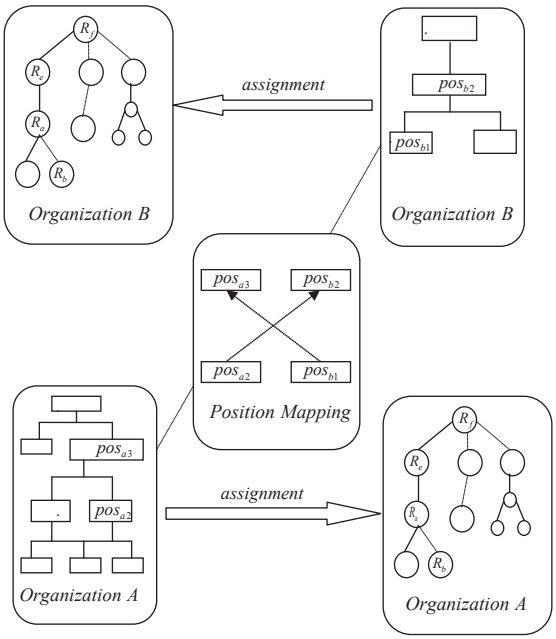

Fig. 8: The position-mapping method in OB4LAC

5 The Acess Operations and Business Collaboration among Multi-Organizations

As we discussed in section 2, RBAC model is more suitable for a single information system environment, when facing the multi-organizations it would make the authorization management of system out of control. OB4LAC model is based on the organization-based access control method, it adopts the method of "Position Mapping" to solve the access operations and business collaboration among multi-organizations and through it to avoid those problems occurred in RBAC Model. As shown in Fig.8, the positions Pos_{a2}, Pos_{a3} in organization A and Pos_{b2}, Pos_{b3} in organization B establish the position mapping relations, so the user u_a which is assigned to Pos_{a2} in organization A would acquire the authorization of Pos_{b2} in organization B. Then we can see that the method of "Position Mapping" does not change the authorization of each position, but only change the access permission of the user assigned to the requesting position in target organization, so this method can avoid expand the authorization of a role that occurred in RBAC model. As already mentioned in the introduction the mathematical model of Dalgaard and Strulik [2] is concerned with the modelling of an economy viewed as a transportation network for electricity. Electricity is used to run, maintain, and create capital.

Definition 11. the position mapping management functions:

If there have positions $Pos_i \in Pos_{p1}$ in organization A and $Pos_j \in Pos_{p2}$ in organization B, then $(Pos_i, Pos_j) \in OAO_{p1,p2} \subseteq Pos_{p1} \times Pos_{p2}$ represents that the position Pos_i establish position mapping relation with Pos_j.

Definition 12. the position mapping authorization function:
If position mapping relation $(Pos_i, Pos_j) \in OAO_{p1,p2}$ has been established, the user u_{p1} which is assigned to Pos_i in organization $p1$ would acquire the authorization of Pos_j in organization $p2$. $assigned\_pos_{p2}(u_{p1}) = \{pos_j \in POS_{p2} \,|\, (pos_i,\ pos_j \in OAO_{p1,p2}),\ pos_i \in assigned\_pos_{p1}(u_{p1})\}$

6 Conclusions And Future Work

This paper first discussed the current problems in RBAC model when facing the multi-level, complex and distributed information systems, and find that the essential reasons are due to the conflict in working pattern between the RBAC model and the physical world. Thus, we propose a new access control method-Organization Based Access Control Theory and its specific model-OB4LAC model, which improve the RBAC model through the approach of adding a layer of "position", so it expand the model's structure from user - role - permission to user - position - role - permission. Then, it changes the core of authorization management from "Role" to "Position", and through the viewpoint of organization management to solve the security problems of access

operations and business cooperation among multi-organizations. This article analyze the constituent members, formal description and sub-models UPA, PORA and PERA of OB4LAC model, and also gives the specific process steps in access operations and business collaboration among multi- organizations. Through the test in many complex E-government systems, OB4LAC model achieves good results. Next, we will focus on the process of OB4LAC model in the temporal constrains, including time constraints, resource constraints, etc., and also would do the deep research about the security issues and risks of OB4LAC model in the access operations and business collaborations among multi-organizations.

Acknowledgement

This research has been supported by the National Natural Science Foundation of China (91024029), China Postdoctoral Science Foundation funded project (2013M540273).

References

[1] Sandhu R. Role Based Access Control Models [J]. IEEE Computer, 38-47 (1996).
[2] Sandhu R. Bhamidipati V, Munawer Q. The ARBAC97 Model for Role Based Administration of Roles [J]. ACM Transaction on Information and System, 105-135 (1999)
[3] S. Oh, Master integrity principle for effective management of role hierarchy [J].Journal of Korea Information Processing Society, **12-C**, 981-988 (2005).
[4] F. Cuppens and A. Mige, "Modeling contexts in the or-BAC model," in Proceedings of the19th Applied Computer Security Associates Conference, 416-427 (2003).
[5] F. Cuppens and A. Mige, "Administration model for or-BAC," in Workshop on Metadata for Security, International Federated Conference, 754-768 (2003).
[6] SEJONGOH, CHANGWOOBYUN, SEOG PARK. An Organizational Structure- Based Administration Model for Decentralized Access Control[J]. Journal of Information Science and Engineering, **22**, 1465-1483 (2006)
[7] R. Sandhu, V. Bhamidipati and Q. Munawer, The ARBAC97 Model for Role-Based Administration of Roles, ACM Transactions on Information and System Security, **2**, (1999).
[8] E. Barka and R. Sandhu, A Role-Based Delegation Model and Some Extensions, Proc. of 23rd National Information Systems Security Conference, (2000).
[9] L. Zhang, G. Ahn, and B. Chu, A rule-based Framework for Role-Based Delegation, ACM Transactions on Information and Systems Security, **6**, 404-4 (2003) .
[10] J. B. D. Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor. A Generalized Temporal Role-Based Access Control Model . IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, **17**, 4-23 (2005).
[11] J. B. D. Joshi, W. G. Aref, A. Ghafoor and E. H. Spafford. Security models for web-based applications. Communications of the ACM, **44**, 38-72 (2001).
[12] J. B. D. Joshi, E. Bertino, A. Ghafoor. Hybrid Tem Role Hierarchies in GTRBAC. Submitted to ACM Transactions on Information and System Security.
[13] YU Miao, WANG Yanzhang. Research on an E-government Affairs System Architecture Based on Role Network Model & Its Realization[J].Computer Engineering and Applications, **39**, 31-35 (2003).
[14] LI Huaiming, Ye Xin, WANG Yanzhang. Organization and Empowerment Management of the Complex Government Affair Information System[J].System Engineering, **24**, 44-48 (2006).
[15] A. Schaad. A Framework for Organizational Control Principles. PhD thesis, The University of York, York, England, (2003).
[16] C. Wolter, H. Plate, and C. Herbert. Collaborative Workflow Management for eGovernment, Accepted in the 1st international workshop on Enterprise Information Systems Engineering(WEISE), (2007).
[17] J. Crampton and H. Khambhammettu. Delegation in role-based access control. In Proceedings of the Computer Security - ESORICS 2006, 11th European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20, 2006, Lecture Notes in Computer Science, Springer, 174-191 (2006).
[18] J. Wainer, A. Kumar, A Fine-grained, Controllable, User-to-user Delegation Method in RBAC, ACM Symposium on Access Control Models and Technologies, Sweden, Jun 1-3, (2005).

You Peng received the PhD degree in Management Science and Engineering at Dalian University of Technology, His Research interests are in the areas of System Engineering, including the information system, decision support system, etc. He has published research articles in reputed journals of information technology and emergency management.

Yan Song is currently a professor in the Economic and Management School at harbin Engineering University, and she is the director of this school. She received the PhD degree in computer science at Harbin Engineering University. Her Research interests are in the areas of System Engineering, including the information system, emergency management, etc. She has published research articles in many reputed international journals.

Hang Ju is Associate Professor of Management science and Engineering at Harbin Engineering University. She was the Founder and Director of Integration of Earned Value Management Laboratory. Hang Ju received the PhD degree in Management Science and Engineering at Harbin Institute of Technology. Her Research interests are in the areas of Project management, Cost engineering, including the Economic analysis, IEVM, Exhibition Economy, Industrial Cluster, etc.

Yanzhang Wang is currently a professor in the Management School at Dalian University of Technology, and he is the director of Information Technology and Decision Support Laboratory. He received the PhD degree in system engineering at Dalian University of Technology. His Research interests are in the areas of System Engineering, including the information system, Decision Support system. He has published many research articles in reputed international journals.