Modeling of RBAC-based access control of virtual enterprise

Dejun Chen
School of Information Engineering, Wuhan University of Technology, Wuhan, People’s Republic of China and
Manufacturing Engineering Centre, Cardiff University, Cardiff, UK

Zude Zhou and Yingzhe Ma
School of Information Engineering, Wuhan University of Technology, Wuhan, People’s Republic of China, and

D.T. Pham
Manufacturing Engineering Centre, Cardiff University, Cardiff, UK

Abstract
Purpose – The purpose of this paper is to create a model of role-based access control (RBAC) based access control for virtual enterprise (VE).

Design/methodology/approach – An access control model for security and management of VE is presented by integrating generic structure of VE and applying the principles of RBAC. In addition, the application of the model to a supply chain-oriented VE illustrates that a general access control scheme can ensure the running of VE.

Findings – A theory base of access control for the realization of the VE is found.

Originality/value – The paper presents a very useful new model of access control for VE. This paper is aimed at researchers and engineers.

Keywords Control technology, Modelling, Virtual organizations

Paper type Technical paper

1. Introduction

There are two traditional technologies of access control, namely discretionary access control (DAC) and mandatory access control (MAC), both of which have their own limitations (Fan et al., 2000). In particular, DAC grants access permission to users directly. However, when the number of users is large and frequently changes, authorization management increases in complexity. In MAC systems, restriction of the access from subjects to objects depends on objects’ sensitivity level and subjects’ permission level. Although MAC reinforces the confidentiality of information, it cannot implement integrated control function. Combination of MAC and DAC allows the access to an object only after the checkout of DAC and MAC is performed on a subject.

Role-based access control (RBAC) is a flexible and effective access control method, whose main principle is to grant access permissions to users by setting up relationships between access permissions and roles first and then by assigning suitable roles to users. In RBAC, role is a permission set, which is related to a specific work.

The authors express their thanks to the International Major Joint Project (50620130441) and the National Postdoctoral Fund (2005037192) of People’s Republic of China for supporting this research.
To change the user access, it is only required to remove and reassign roles. RBAC can effectively avoid the disadvantages of traditional access control, and reduce the complications of authorized management as well as management cost. As an effective access control method (for recent discussions on general control problems, refer to Lin (1987, 1990) and Lin and Ma (1990)), RBAC has been widely investigated and several extensions have been proposed (Bertino, 2003).

With the blooming development of network technology, network-based digital manufacturing system, whose basic organization form is virtual enterprise (VE), appeared rapidly. VE is a temporary enterprise union, in which several independent enterprises share their resources and are connected with network information technology (Chen et al., 2006). Owing to importance of enterprise data commuted, the safe information transport methods have been researched widely (Zhao and Wang, 2002; Chen et al., 2006). How to implement the access control of all kinds of users under the new enterprise organization and management mode, it has also become the researching hotspot in recent years. In literature (Chen et al., 2007), the access method based on RBAC has been studied extensively, however, it has not been considered in a general VE model. For this reason, a general construction model and its requirements for access control are analyzed in this paper. Then, a RBAC model named VE-RBAC is proposed. Finally, the application of the model in VE is investigated.

2. The general structure and access requirement of VE
Unlike traditional enterprises, VE does not have fixed entity components. However, from the process of establishment and operations of VE, some key components can be extracted, namely alternative competence team (ACT), virtual working team (VWT) and virtual affairs cooperative center (VACC). According to these components, a two-level organizational structure model has been presented (Chen et al., 2006). Here, ACT is an alternative enterprise (AE) set determined by evaluation on core competence of bidding enterprises from central enterprise after introducing public bidding to assignment of tasks of VE. Each sub-task of VE matches a core competence. Every core competence is relevant to several AEs. Obviously, the enterprises in ACT are redundant to effectively respond to the risks that take place in key procedures. VWT is the work group, after the task is divided into some sub-tasks based on the requirements of different periods, optimally assembled by the members of ACT according to some guidelines, such as cost, time, etc. Every subtask matches a member enterprise (ME). VACC is the management department of a virtual organization, which is in charge of the cooperation, supervision, direction and outward contacts of ACT, VWT and the whole organization network. It can be regarded as the integration of directorate, managers, and some other office roles in an entity organization.

On one hand, although the organization structure of VE differs from entity enterprise, building a VE consists in grouping different participant entity enterprises in order to achieve the behavior of a normal enterprise. However, goals and requirements of access control do not change, and its basic method can be applied on VE as well. On the other hand, the relationships between the constituting VEs are temporarily and dynamic, they are different from those between headquarters and branches. When the situation changes, their relationship of alliance will also change or terminate and they may become opponents. Thus, every entity enterprise must ensure
the security of its own sensitive information during the period of cooperation while sharing resources. As a result, the method of access control becomes very complicated.

Except for the similar demands of management functions between VACC and entity enterprises, from the previous session about organization structure of VE, the valid permissions of relevant users in ME and ACT have their own characteristics. This changes department classification, management goals, categories of operation, operators and their properties. Therefore, the operation set and objects within the whole VE has to be analyzed and designed, a new reasonable and common access control method has to be built.

The diagrams of information storage and function distribution of VE shown in Figure 1 illustrate the operation and management functions of VE. In this figure, VACC achieves some functions related to the data center of VE, such as analysis of market information and bidding results, establishment of the goal plan, task assignment and implementation of schedule and risk monitoring. In addition, based on the permission of roles, the information of every member in AE and ME can be accessed, such as searching the storage of ME and status information of AE. According to requirements of cooperation between members and based on the local database, MEs can implement storage and access of schedule information which is assigned to its sub-task, cooperation design between MEs and relative storage management functions. AEs have a waiting status in the whole period of VE operation, and their current state

Figure 1.
Information storage and function distribution of VE
information is focused by VACC. Thus, AEs must update and upload their relative status information in local databases.

Based on the above centralization and distribution of storage information distribution, combining of the process of organization management, General access control model of VE can be established after constructing corresponding role set, operation set and object set.

3. Modeling of access control of VE

According to the analysis for the distribution of storage information and requirement of function described in the previous section and to the structure of the RBAC model (Qiuwei et al., 2006), three relevant sets, namely role set, operation set and object set, can be defined. There are three types of role sets of VE, which are VACC member, VWT member and ACT member. They belong to different organization modules. The three types of role sets can be denoted as \( V \), \( W \), and \( T \), respectively, so the role set of the whole system can be expressed as \( R = \{V, W, A\} \). Object sets contain the data objects of VACC, VWT and ACT that are distributed in different domains, and VWT and ACT also contain data objects of different enterprises. If the three types of object sets are denoted as VOBJ, WOBJ, AOBJ, the object set of whole system can be expressed as follows:

\[
OBJ = \{VOBJ, WOBJ, AOBJ\}
\]

To match the objects and roles above, regarding a group of operation set, the permissions will be set up between the operations on \( OP \) and \( OBJ \), expressed as follows:

\[
P = OP \times OBJ
\]

Permission allows the operation on one or more objects. The permissions above refer to concrete objects belonging to the domain of VACC, VWT and ACT, respectively.

The structure of every element of VE permission is defined, but the relationship between them cannot totally follow the method of RBAC. For instance, according to the relationship of role elements in literature (Qiuwei et al., 2006): \( RH \subseteq R \times R \), the relationship expressed as \( \{V, W, A\} \times \{V, W, A\} \) is obtained. However, according to the organization structure of VE, a user can only belong to any of \( V, W \) and \( T \), not the combination of them. That is to say, it only allows arrangement of the role levels of VE in their own organization. The changes of above relationships will affect the priority of session and PRI of user access. Therefore, the components of the module of RBAC model must be redefined to obtain the general definition of RBAC-based VE access control model (VE-RBAC).

**Definition 1.** The model structure of VE-RBAC is shown in Figure 2. The components of module in this figure are defined as follows:

- \( U \) is the user set, which is expressed as \( U = \{u_1, u_2, \ldots, u_n\} \).
- \( R = \{V, W, A\}; \) \( V \) is the role set of VACC. \( W \) is the role set of VWT. \( A \) is the role set of ACT.
- \( OBJ \) is the object set, which is expressed as \( \{VOBJ, WOBJ, AOBJ\} \) where, VOBJ is the object set of VACC, which is expressed as \( VOBJ = \{obj_{V1}, obj_{V2}, \ldots, obj_{VM}\} \).
WOBJ = \{OBJ_{W1}, OBJ_{W2}, OBJ_{WN}\} \\
= \{\{obj_{W11}, ..., obj_{W1T1}\}, \{obj_{W21}, ..., obj_{W2T2}\}, ..., \{obj_{WN1}, ..., obj_{WNn}\}\}

is the object set of different enterprises in VWT and:

AOBJ = \{OBJ_{A1}, OBJ_{A2}...OBJ_{AL}\} \\
= \{\{obj_{A11}, ..., obj_{A1l1}\}, \{obj_{A21}, ..., obj_{A2l2}\}, ..., \{obj_{AL1}, ..., obj_{ALll}\}\},

is the object set of different enterprises in ACT.

- RH\{V \times V, W \times W, A \times A\} is the relationship between role factors in different role sets or a partial order of role level, expressed by \(\succeq\).
- OP is operation set, which is expressed as \{op_{1}, op_{2}...op_{n}\}.
- P = OP \times OBJ, is permission set and is expressed as \{p_{1}, p_{2}...p_{n}\}.
- PA \subseteq P \times R = OP \times OBJ \times R, is the distribution relationship between role and permission, which is a multi-to- multi relationship.
- UA \subseteq U \times R, is the distribution relationship between user and role and a multi-to-multi relationship.
- S is session set, which is expressed as \{s_{1}, s_{2}...s_{n}\}.
- User, is the user set and denotes \(R \rightarrow 2^{U}\), mapping every role to a group of users. So:

\[
\text{User}(r_{i}) = \{u \in U|(u, r_{i}) \in UA\}
\]

- Roles denotes \(S \rightarrow 2^{R}\), which is the function to mapping session to a role set:

\[
\text{Roles}(s_{i}) = \{r \in R|(u_{i}, r) \in UA\}
\]

every \(s_{i}\) has the permission that is:

\[
\bigcup_{r \in \text{Roles}(s_{i})}\{p| (p, r) \in PA\}
Roles’ denotes $S \rightarrow 2^R$. It expands the roles while applying role level as follows:

$$\text{Roles}'(s_i) = \{r \in R | (\exists r' \equiv r)[(u_i, r') \in UA]\}$$

Every $s_i$ has the permission that is:

$$\bigcup_{r \in \text{Roles}(s_i)} \{p \in P | (\exists r'' \equiv r)[(p, r'') \in PA]\}$$

Here, $r, r', r'' \in V$ or $r, r', r'' \in W$ or $r, r', r'' \in A$

- Permissions denotes $R \rightarrow 2^P$, which is the function to mapping every role to a group of permission. So:

$$\text{Permissions}(r_i) = \{p \in P | (p, r_i) \in PA\}$$

Permission’ denotes $R \rightarrow 2^P$. It expands the roles while applying role level as follows:

$$\text{Permissions}'(r_i) = \{p \in P | (\exists r' \equiv r_i)[(p, r') \in PA]\}$$

Where, $r, r', r'' \in V$ or $r, r', r'' \in W$ or $r, r', r'' \in A$

- Constraints are a group of constraints to determine whether to accept the former parts of VE-RBAC model or not, and contain all the present constraints in RBAC. The later operation can be performed after the former conditions are accepted.

The objects and users of distributive storage are added to the model above, and the complex relationship between them is they well interpreted and restricted. Based on the model above, the access control rules of VE system can be defined.

4. Implementation
Based on VE-RBAC, we will discuss on the access control to supply chain-oriented VE. A VE manufactures different series of wine based on market demands. VACC is in charge of the whole process from discovery of market opportunity to establishment and management of the whole VE. VWT includes supplier, manufacturer and franchiser located in Guizhou, Guangdong and Shanghai, etc. Relying on internet, the operations of the enterprise are shown in Figure 1. In practice, the VE-RBAC model is applied. Especially, for MEs in VWT, their different business types lead to different roles.

Table I shows that, managers and storehouse administrators are the common roles in the three types of enterprises. Nevertheless, because they are in different types of enterprises, they hold different permissions. This is $W$ that contains all the aforementioned roles and assign the permissions through PA to ensure that content and amount of storage, but not cost, is available for the storehouse administrators in different enterprise to view. However, authorized operations and searches are available in their own enterprise, such as input and output warehouse amount. The manager inherits the permissions of other roles in his own enterprise based on constraints of role hierarchy and inheritance.

The roles in VACC include cooperative center commissioners, accountants, manufacture supervisors and warehouse administrator. If a user plays the role of warehouse administrator, he or she only belongs to VACC instead of VWT no matter which ME he or she comes from. The warehouse administrator can obtain the storage...
information of all MEs to make records. Therefore, the right operations on the complex relationship of users, roles and objects with UA, PA, and RH can be performed.

The role authorization strategy mentioned above has been implemented in Kweichow Moutai Co., Ltd. Similarly, the other authorization strategies sets to task, enterprise, relationship of enterprise, VACC will be realized in the following works. Finally, the access control strategy of the whole VE will be formed.

5. Conclusion
Traditional RBAC provides a one-entity-enterprise-oriented access control method, but cannot fit the environment of VE completely. As a special enterprise, VE has higher requirements for information security. By combining the traditional RBAC model, with the general organization and running structure model, this paper rebuilds elements and relationship between them in RBAC model, to form the VE-RBAC model that satisfies all styles of VE. In addition, the application of this model is illustrated by a concrete example. In the future, combined with workflow engine of VE (Chen et al., 2006), the whole system of VE will be implemented.

References

**Corresponding author**
Dejun Chen can be contacted at: mrchendj@hotmail.com

To purchase reprints of this article please e-mail: reprints@emeraldinsight.com
Or visit our web site for further details: www.emeraldinsight.com/reprints