# Application of Role-Based Access Control Model in High-Level Athletes Management System

Yijun Li
Department of Physical Education, Central South University, Changsha, 410083 China

***Abstract*—Aimed at that there are large numbers of users visiting high-level athletes' management system, the control model of traditional access can't fully meet the weaknesses of these requirements, proposing the idea of multi-rights management based on ARBAC02 model and establishing a new rights management system. Practice result shows that this strategy can substantially enhance the flexibility and security of access control and provide some reference for digital physical education.**

***Keywords-physical education; information management; access control***

## I. INTRODUCTION

Scientific management of high-level athletes is an important part of physical education in the management, high-level sports team management information not only enables the competent leadership of high-level athletes and coaches to conduct a comprehensive and timely information to understand, but also at any time helps coaches to develop a training program for different high-level athletes, coaches make more systematic training of high level athletes, rationalize and enhance high-level coaches for athletes training. Due to that high levels of operational staff management system user identity involves many athletes, coaches, administrators and other systems, using a different identity for the purpose of the system is not the same, at the same time and under the same identity it is as a result of differences in sports system access existing difference, so how to make different visitors have different access rights to run at a high level member of the management system is an important issue of access control systems. With access to control technology continues to evolve, it has appeared in different access control model and applied to various information systems, traditional access control models are mainly discretionary access control (DAC, discretionary access control) model, mandatory access control (MAC, mandatory access control) model [1,2]. Appropriate resource access control policy is a guarantee of security, a high level of operational staff management system is significantly different from the existence of a multi-user multi-role, since the main traditional DAC and MAC access control model is to explore the subject (Subject) which has permission to deposit take receptor (Object) relationship, and therefore it can not be considered in the rights management to differences between subjects, and recently it has been widely used in the role-based access control (RBAC, role-based access control) model [3] which can overcome shortcomings of traditional access control model.

## II. ROLE-BASED ACCESS CONTROL MODEL

Role-based access control system means the user is assigned to the appropriate roles, and accessing to resources is determined by the respective roles. The model is based on the first proposed by Ferraiolo and Richard. Kuhn and other scholars, and later is through Sandhu and other scholars to be improved, the US National Institute of Standards and Technology (National Institute of Standards and Technology, NIST) are to be incorporated by the organization, after finishing order fixed standard, it is called NIST RBAC, as shown in FIG.

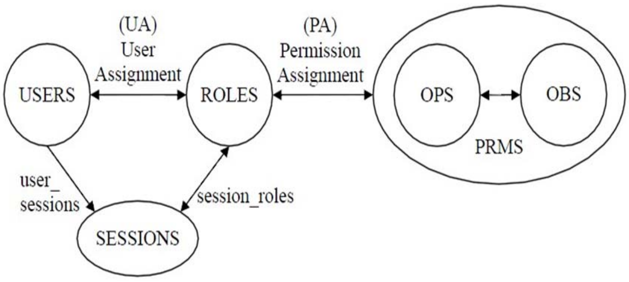

Figure 1. Role-based access control model

ARBAC02 model is to improve and optimize the RBAC model, which has been showed in Figure 2. It consists of three sub-models: the privilege - Management Role Management Model (PRA, Permission-Role Assignment), the relationship between the model and the role is of responsible privileges; user - role management model (URA, User-Role Assignment), the model is responsible for managing the relationship between users and roles; Role management Model (RRA, Role-Role Assignment), the relationship between the role of the model is responsible for the generation and management of roles.

When permission administrator makes permissions management, he takes into account the fact that the system in each organizational unit in order to complete a feature many users and have the appropriate permissions, ARBAC02 model established two independent organizational structure (organization structure), one is called pool users (OS-U, organization structure-user), another pool is called permissions (OS-P, organization structure-permission). In the user pool, each organizational unit is pre-defined roles feature; in the pool privileges each organizational unit is included for the realization of this function has a range of privileges.

(Meaning RBAC model is the "Role-based access control model", RBAC is the abbreviation, full name: Role Based Access Control)

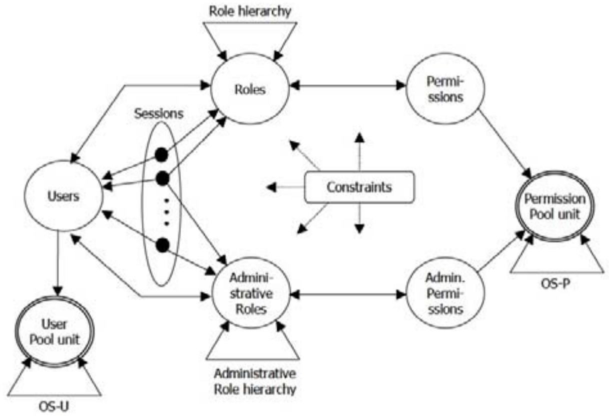

Figure 2. ARBAC02 model structure diagram

In addition to the above features of ARBAC02 model, the biggest difference between it and other access control model is to increase the management of permissions managers, decentralized authority management strategy, there are several rights management roles (administrative role), rights management roles in the same system inheritance relationship which have tree system. In such a huge organization, with many users and roles system, it can be more detailed, flexible resource access control.

## III. Application of Access Control Model Based on ARBAC02

### A. Design of the body

In order to run a natural tissue effectively, it is usually organized in a tree structure planning, and it is organized according to their job function and again subdivided into different subordinate organizations, each of them is responsible for a particular job function, and the user in their organization plays a role to complete a work of the organization, from the access control point of view, the tree structure can be done not only for their organization based rights management personnel, but also has become the basis for the organization of the division of authority. High-level athletes' management system is a typical tree structure, as shown in Figure 3:

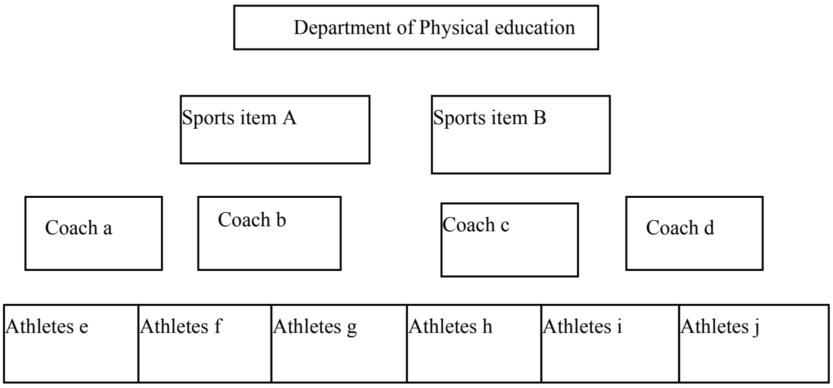

Figure 3. Structure example of high-level athlete management organization

High-level athlete management organizational structure is as the main one has a layered structure and object collection, the role of this collection has some authority to operate within the specified user for this operation and they are shared within this collection, and it can't be outside the organization unit enjoyed by other subjects. Whereby the role definition: if there is a relationship type org (Org, Rol / Org '), called the role Rol or organization Org' belong to organizations Org.

By definition, each organization is defined as an organizational role, the entire organization is defined as the root domain, each subordinate organization is defined as a child role, as pyramid hierarchical organizations constitute the domain tree. For each role domain, there is one or more sub-domain, 0 or a parent role domain. No parent domain is the root domain role domains, and each organization has one and only one root domain.

A domain is a tree structure inherited role is to meet reflexive, transmission and asymmetric three properties is a partial order. In addition to the root node, each system has one and only one root domain, and each domain has one and only one role or no parent, if RH represents the set of all roles domain, the formal expression is:

(1) $RH \subseteq RD \times RD$ RH represents partial order on the set, denoted $\succcurlyeq$, $r1 \succ r2$ represent r1 r2 is a sub-domain, $r1 \succcurlyeq r2$ expressed $r1 \succcurlyeq r2 \vee r1 = r2$, $r1 \succ\succ r2$ expressed r2 r1 is the direct subdomain

(2) $\forall r1, r2, r3 \in RD$, then $r2 \succ\succ r1 \wedge r3 \succ\succ r1 \Rightarrow r2 = r3$

According to high-level athletes under the general functions of the management system for each organization, the paper will be organized to introduce the basic steps

ARBAC02 model structure, the establishment of the role are:

(1) Create a basic role and organization. Since the access control is in practical applications, system privileges different roles in different tissues obtained is not the same, and therefore first needs to divide the basic organizational roles and users of the system based on the use of different purposes, different roles and different organizations have different access control policy. .

(2) The establishment of a multi-level set of organizational roles. On the basis of set of classes and object classes through inheritance to establish the role and organization structure according to the system features object.

(3) Determination access. When a user initiates a guest operating access, the system will first analyze the user through the activation of the role of the session searches for the operation requested by the user object and all objects of the class to which it belongs; and finally whether the role owns the object or the object class operating authority if the object of the operation is by the user on request and user did not reject the request for the object of the operation.

### *B. Object Design*

High-level athletes include a variety of information management system object athletes, athletes such as name, age, training programs, previous training and competition results, etc. So if the management of their individual permissions for each will be very cumbersome. Through analyzing of the object, the information are divided into different sets based on high level athletes and different attributes, each set of objects, a set has the operating authority of the user for this operation within the specified shared system, while they are able to the other main unit outside the organization enjoyed in Figure 4. It can define the object: If there is a relationship type obc (obc, obj / obc '), it indicates that the resource or object ob obc' belong to the object obc.

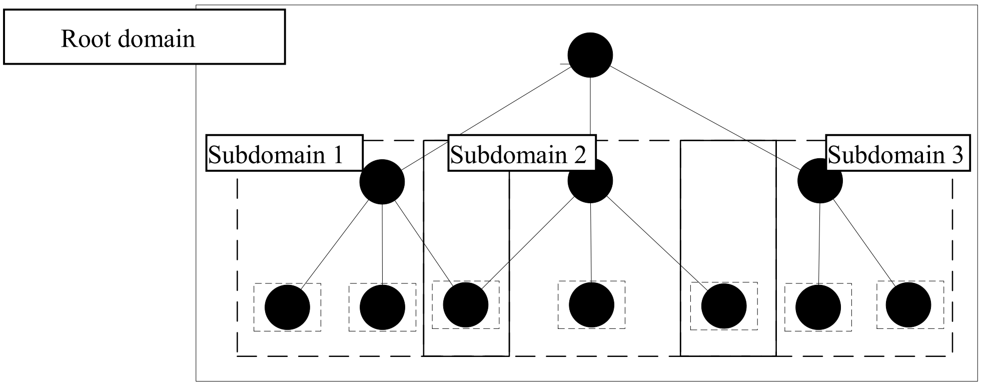

Figure 4. Object Hierarchy

The object also inherits a tree structure which is similar to the role, but not for partial order, each resource belongs to an object class, a collection of object classes is for the resource, if OBC category represents a collection of objects, the formal expression is:

(1) $\forall obj \in OB, \exists obc \in OBC, obj \in obc$

(2) $\forall obc \in OBC, obc \subseteq OB$

According to the information management system under high-level athletes entering the basic information for each athlete, the paper introduced the basic idea ARBAC02 object model:

(1) The object abstraction resolve deficiencies ARBAC02 model which is not high degree of abstraction, object as an abstract object will have a lot of common attributes grouped into a collection, so that they can have the same operational behavior, but the role is different and is mapped many relationship between objects and object, an object class can contain multiple objects and at the same time an object can belong to more than one object class.

(2) Have the inheritance relationship between the object and the object, thus further improving the degree of abstract object classes is easier to multi-level object structure, relationship managers can better handle permissions between subject and object.

(3) Access to the object manager can define permissions, permissions on an object definition for the object is not only effective, but also applies to all objects belonging to the object, so that it is not only beneficial to assign permissions flexibility while improving the competence distribution of efficiency, it can reduce the number of permissions assigned.

### *C. Implementation Process Rights Management*

Figure 5: improved ARBAC02 model management system in high-level athletes rights management flowchart. The steps are as follows:

Step 1: System privilege management roles apply for resource authorization privileges to the role of resource owners

Step 2: The system determines resource type according to the context

Step 3: The system user rights management roles and resources develop appropriate role-based access control policies based on resource type

Step 4: The system privilege management role develops good after successfully authorized access control policies for resource management authority

Step 5: The role of the resource owner refuses to authorize the authorization fails, as it is still authorized permission to re-start the authorization process.

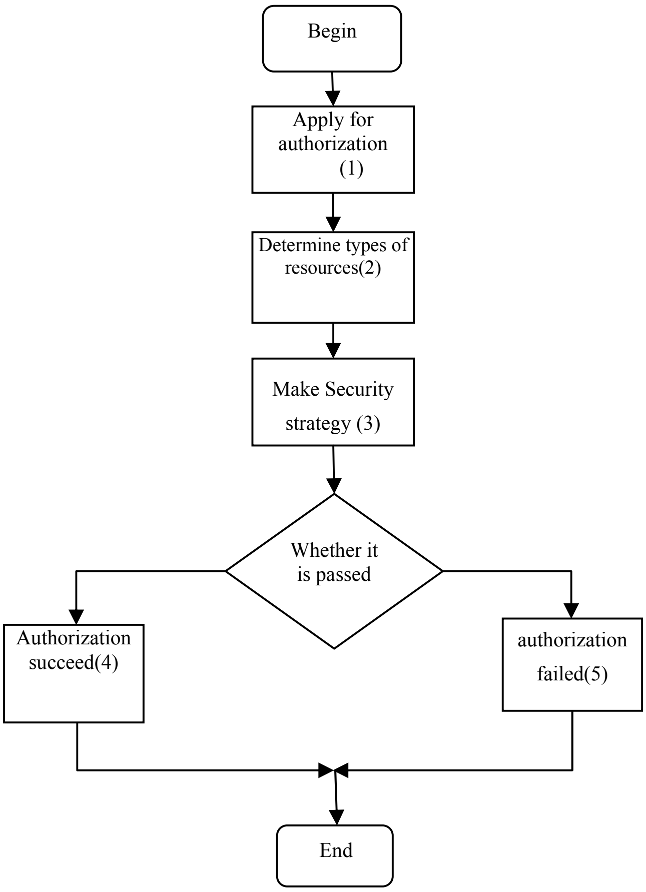
Begin
Apply for authorization (1)
Determine types of resources(2)
Make Security strategy (3)
Whether it is passed
Authorization succeed(4)
authorization failed(5)
End

Figure 5. Flowchart authorized certification authority

Through analyzing it shows that rights management processes comply with security controls two principles:

Principle of least privilege: the role of rights management systems can only apply for authorization permissions required, if delegated authority beyond their roles, the role of the resource owner may refuse permission to apply for authorization. When the system privileges change the role of task management roles have permission to be resumed the role of the resource owner.

The principle of separation of duties: When authorized by the behavior of some systems require different authorization rights management roles, such as the role of coaches having administrative privileges to be coaches and management role must be different. This can be achieved through the development of security policies apply when delegated authority.

## IV. Conclusions and Prospects

Different from traditional access control policies, improved access control policy is so greatly enhanced access control flexibility, the system can develop different access control policy, and full express the wishes of the system's security systems for different visitors. At the same time due to the access control policy is through role rather than a direct effect on the object, instead of reducing the burden of system management and maintenance, we can improve work efficiency. Because of role-based access control model is still a coarse-grained access control model, when the main access to the system is long enough to still cause complex permission check, how to refine the operation of object granularity of control by the time period reflected in the data features to improve the competence of calibration efficiency and it will be the direction of future research.

## References

[1] Department of Defense. Trusted computer system evaluation criteria (TESEC)[S]. Technical Report, DOD 5200.28-STD, 1985.

[2] L Snyder. Formal Models of Capability-based Protection Systems[J].IEEE Transactions on Computers, 1981, 30 (3) : 1722181.

[3] Sandhu R, Coyne EJ, Feinstein HL, Youman CE. Role-Based access control models[C]. IEEE Computer, 1996,29(2):38−47.

[4] Thomas RK, Sandhu RS. Task-Based authentication control (TBAC): A family of models for active an enterprise-oriented authentication management[C]. In: Proc. of the 11th IFIP Conf. on Database Security. California, 1997. 11−13.

[5] Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 model for role-based administration of roles[C]. ACM Trans. on Information and System Security (TISSEC), 1999,2(1):105−135.

[6] Ferraiolo DF, Sandhu R, Gavrila S. Proposed NIST standard for role-based access control[C]. ACM Trans. on Information and Systems Security (TISSEC), 2001,4(3):224−274.

[7] Oh S, Sandhu R. A. Model for role administration using organization structure[C]. In: Sandhu R, Bertino E, eds. Proc. of the 6th ACM Symp. on Access Control Models and Technologies (SACMAT 2002). Monterey: ACM Press, 2002. 155−162.

[8] Kalam A A E, Baida R E, Balbiani P, et al. Organization based access control Proc[C]. of 4th IEEE International Work shop on Policies for Distributed Systems and Networks. 2003: 120-131.