RESEARCH ARTICLE OPEN ACCESS

Modeling Level Wise Role-Based Access Control for Commercial Database Systems

Trilochan Tarai[1], Pradipta Kumar Mishra[2]
Department of Computer science & Engineering, Centurion University of Technology & Management Bhubaneswar, India

Abstract
Now a days database system is becoming more crucial as the scale of database is growing. Traditional access control policies have certain disadvantages. So as a promising alternative to traditional access control policy, Role-Based Access Control (RBAC) has received special attention for its unique flexibility. RBAC provides access control based on permissions associated with roles. Among commercial software applications, DBMS provide access control and have applied RBAC. But RBAC have also certain inherent weaknesses. So in this paper we enhance the RBAC policy named as Level Wise Role-Based Access Control (LWRBAC) policy that is instead of access control through role assigned to the users, the users are assigned by some level of access control and it can implement in object relational databases in order to develop secured software applications.
Keywords- RBAC, LWRBAC.

I. Introduction

Role-based Access Control (RBAC) has attracted considerable attention as an alternative to traditional Discretionary Access Control (DAC) and Mandatory Access Control (MAC). RBAC has been widely researched and received attention and capability list schemes. Basically a role-based access control model is involved with users, roles, sessions, operations, objects, and role hierarchy. A user has access to an object based on the assigned role. A role is a group of users that have the same job functionality within an organization. Roles access resources based on policies or role rights. The object is concerned with the user's role but not the user. Users frequently change but not the roles, which makes RBAC a better access control mechanism[3][4][12]. Permission is an approval to perform an operation on objects. A session contains a set of roles that can be activated by a user during a period of time. One advantage of using RBAC is that the implementation of access control will be more reliable than the traditional ones.

The remaining part of the paper is organized in the following way : related work is discussed in Section 2. In Section 3, we briefly introduce the concept of Level Wise Role-Based Access Control(LWRBAC). In Section 4, a role assignment algorithm is presented to implement LWRBAC. Finally the paper is concluded in Section 5.

II. Related Work

Role-Based access control has been well recognized for providing more advantages than traditional access control[2][7][10] schemes. A family of reference models has also received support as generalized approach to role-based access control[10][11]. Several attempts to implement role-based access control have been made using programming languages or commercial database management systems[3][10]. The RBAC features and policies include user role assignment, role relationships, constraints and assignable privileges. Not surprisingly, it appears that none of the commercial database management systems support the entire features and policies of role-based access control. Oracle fully supports the user role assignment and assignable privileges, but it is very weak in role relationships and constraints and assignable privileges. The features and policies of Sybase is somewhere between Informix and Oracle. A formal specification of access control policies allows us to investigate whether a system preserves security policy invariants across the state changes or not[13].In RBAC one question is arising that "Is the RBAC policy is enough for expressing access control policies" ? If the answer is no, then what will be done to improve the model. We assume that each organizations has administrators to establish, enforce and manage policies in access control. We handle the RBAC policy in application programs. Application programs implement the constraints based on individual organization's access control policies. If same role will be assigned to multiple users through the application programs, then the code complexity will be increased.

III. Level Wise Role-Based Access Control

We have enhanced the RBAC policy in order to reduce the complexity of role assignment task of administrator by eliminating redundant assignment statements associated in basic RBAC model. In this policy, an administrator defines and creates a set of levels by taking a user or a set of users. Then different roles are assigned to the levels according to the role hierarchy of organization. Here level is mapped to the role instead of users for accessing the resources. So for this point of view we have presented this policy as Level Wise Role-Based Access Control (LWRBAC)policy.

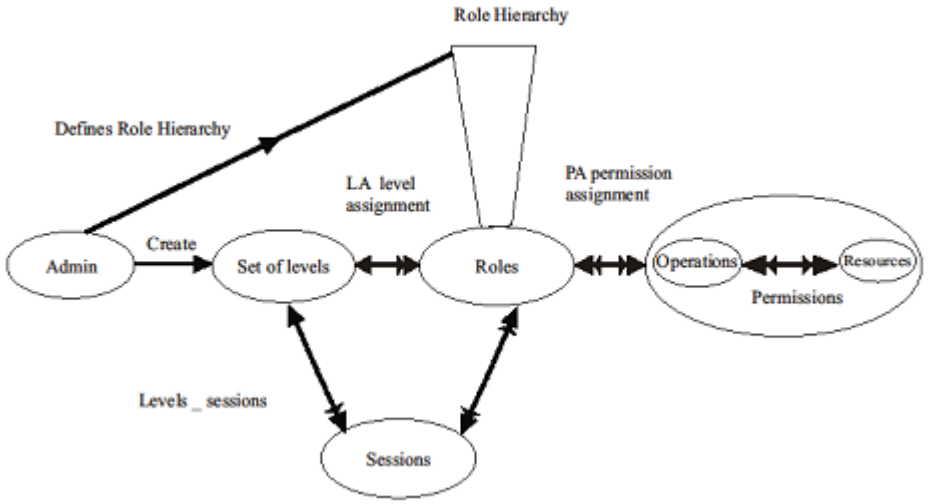

Figure 1. LWRBAC model

This model is based on three sets of entities called levels(L), roles(R), and permissions(P). A set of users created by admin forming a group is identified as a level. A role is a job function or job title within the organization. The Level Assignment(LA) and Permission Assignment(PA) are both many to one relationship. A level can be a member of many roles, but a role can have one level. There is a partially ordered role hierarchy RH, also written as >= where x>=y signifies that role x inherits the permissions assigned to role y. Each session relates one level to possibly many roles. A level establishes a session during which the level activates some subset of roles that he or she is a member of directly or indirectly by means of role hierarchy[1][5][6].

IV. Algorithm for Role Assignment to Levels

Input : level-id: identification of the user level applied task roles
Output : authorize task role set T to the level.
{
for(each task-role A in the applied task-roles)
{
if(task-role A satisfies the level constraints)
{
assign role A to the level L;
}
else
return the refuse message for the application of task role A to the level
}}

V. Conclusion

Role Based Access Control(RBAC) provides more efficiency in access control than traditional access control. A reference model is presenting the basic concept policies and behaviors of role-based access control. Since RBAC as a promising alternative to traditional access control schemes, but it have certain weaknesses that is the complexities of the code for assigning the role to each users. So in this research we made attempt to enhance the RBAC policy and presented as Level Wise Role-Based Access Control(LWRBAC) policy to reduce the complexity of code. We also presented a role assignment algorithm for LWRBAC to develop secured software applications.

References

[1] Betrino Elisa and Sandhu Ravi,"Database Security-Concepts, Approaches, and Challenges", IEEE Transactions on Dependable and Secure Computing, Vol.2, No.1, January-March 2005.
[2] Marius ConstantinLeahu, Mare Dobson, and Giuseppe Avolio, "Access Control Design

and Implementation in the ATLAS Experiment", IEEE Transactions on Nuclear Science, Vol.55, No.1, February 2008.

[3] Anil L. Pereira, VineelaMuppavarapu and Soon M. Chung, "Role-Based Access Control for Grid Database Services Using the Community Authorization Service", IEEE Transactions on Dependable and Secure Computing, Vol.3, No.2, April-June 2006.

[4] Ravi S. Sandhu, Edward J. Cope, Hal L. Feinstein, Charles E. Youman, "Roll Based Access Control Models", IEEE journals, February 1996.

[5] Feikis John, "Database Security", IEEE Journals, February-March 1999.

[6] Ravi S. Sandhu and PierangelaSamarati, "Access Controls Principle and Practice", IEEE Communication Magazine September 1994.

[7] Akshay Patil and B.B.Meshram, "Database Access Control Policies", International Journal of Engineering Research and Applications, Vol.2, May-June 2012.

[8] Min-A Jeong, Jung-Ja Kim and Yonggwan Wan, "A Flexible Database Security System Using Multiple Access Control Policies", IEEE Journals, November 2003.

[9] D.Ferraiolo et al., "Proposed NIST standard for role-based access control", ACM Trans. Inf. Syst. Security, vol.4, no.3, pp.224-274, Aug,2001.

[10] Mark Strembeck and Gustaf Neumann, "An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments," ACM Transactions on Information and System Security, Vol.7, No.3, August 2004, pp.392-427.

[11] Somesh Jha, Ninghui Li, Mahesh Tripunitara, Qihua Wang, and William Winsborough, "Towords Formal Verification of Role-Based Access Control Policies," IEEE Transactions on Dependable and Secure Computing, Vol.5, No.2, April-June, 2008.

[12] Chia-Chu Chiang and Coskun Bayrak, "Modelling Role-Based Access Control Using a Relational Database Tool", IEEE IRI 2008, July 13-15, 2008, Las Vegas, Nevada, USA.

[13] D. Mc Pherson, Role-Based Access Control for Multi-Tier Applications Using Authoriza-tion Manager, Retrieved from http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/athmanwp.mspx, 2008.