International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967 *Volume 2 , Issue 1(Jan-Feb 2015), PP1-5*

Modeling Level Wise Role-Based Access Control Using a Relational Database Tool

Trilochan Tarai

Department of Computer Science & Engineering, Vivekananda Institute of Technology, Bhubaneswar, India

Abstract :-Now a days the role of a database system is very crucial for any enterprise. Traditional access control policies such as Mandatory Access Control(MAC), Discretionary Access Control(DAC) have certain weaknesses. Another traditional access control policy that is Role-Based Access Control(RBAC) is a promising alternative traditional access control policy, which 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 we use a relational database tool called Oracle to study the behavior of a level wise role-based access control model. A detailed discussion of the level wise role-based access control behaviors and policies is then presented.

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 [2][5][11]. 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 II. In Section III, we briefly introduce the concept of Level Wise Role-Based Access Control (LWRBAC). In Section IV, we study the behavior of LWRBAC model. A database tool is used to create a prototype for experimentations. Finally the paper is concluded in Section V.

II. RELATED WORK

Role-Based access control has been well recognized for providing more advantages than MAC and DAC schemes [2][7][10]. A family of reference models has also received support as generalized approach to role-

based access control [10][12]. 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. 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 organization 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, definitely the code complexity will be increased. So this is a major disadvantage of RBAC.

III. LEVEL WISE ROLE BASED ACCESS CONTROL

We 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 according to the mapping of role to the level, we named the policy as "Level Wise Role-Based Access Control (LWRBAC) Policy. The following figure1 is representing the model of LWRBAC.

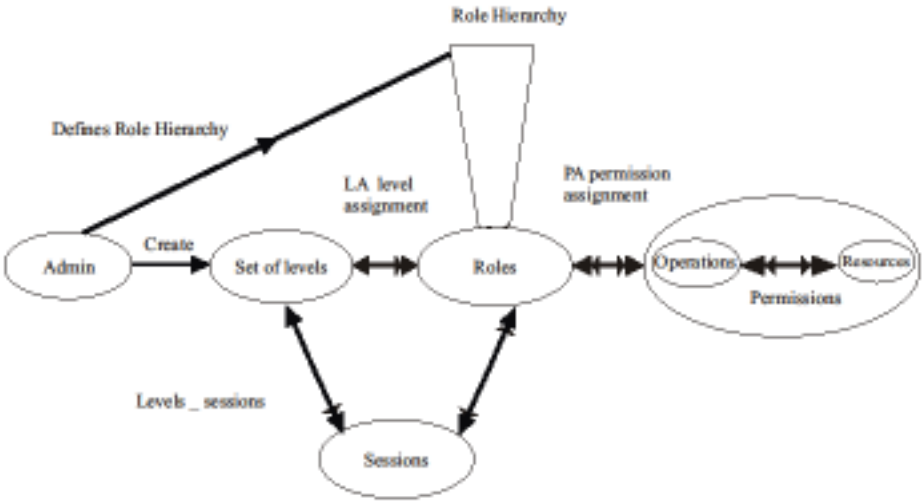

Fig 1. LWRBAC model

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.

IV. A CASE STUDY FOR DESIGNING LWRBAC

Here, we present a Case Study by using a relational database tool called Oracle 10g to study the behavior of Level Wise Role-Based Access Control.

Administration Query: User Abinash is the administrator. He owns the database. So the required SQL query for administrator is :

CREATE USER Abinash identified by abc;

GRANT create user, create session TO Abinash with ADMIN OPTION;

GRANT dba to Abinash;

The following relational tables are required for our Case Study:

create table user_permission (user_id varchar2(15), user_name varchar2(12), code_no number(12));

create table user_level (level_namevarchar2(12), code_no number(12));

Here we have defined a procedure to study the behavior of LWRBAC model.

```
create or replace procedure p1
is cnt number(4) ;
cursor c1 is
select user_name from user_permission , user_level
where user_permission . code_no = user_level.code_no ;
begin
select count(user_name) into cnt from user_permission , user_level where user_permission . code_no = user_level.code_no ;
dbms_output.put_line(cnt);
for rec in c1
loop
EXECUTE IMMEDIATE ' grant create session to ' || rec . user_name;
EXECUTE IMMEDIATE ' grant role1 to ' || rec . user_name;
dbms_output.put_line(rec.user_name);
EXECUTE IMMEDIATE ' grant select , insert on v1 to ' || rec . user_name;
end loop;
end p1;
```

V. CONCLUSION

Traditional access control schemes have strong couplings between users and operations, but Role Based Access Control (RBAC) provides more efficiency in access control than traditional access control. Since RBAC as a promising alternative to traditional access control schemes, but it have certain disadvantages that is the complexities of the code for assigning the role to each users. So in this research we made attempt to create a policy by enhancing RBAC called as Level Wise Role-Based Access Control (LWRBAC) policy and present to model the behaviors of level wise role-based access control using a relational database tool called Oracle10g to reduce the complexity of code. We also examined the way a standard LWRBAC can be used to support LWRBAC policies in practice.

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] 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.

[3] 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.

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

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

[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] 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.

[12] 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.

[13] 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.McPherson, Role-Based Access Control for Multi-Tier Applications Using AuthorizationManager,Retrievedfrom http://www.microsoft.com/technet/prodtechnol/ windowsserver2003/technologies/mamagement/athmanwp.mspx, 2008.