Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 73 (2014) 26181-26184

ISSN: 2229-712X

Enhancing database access control policies

Trilochan Tarai and Pradipta Kumar Mishra

Department of Computer science & Engineering, Centurion University of Technology & Management, Bhubaneswar, India.

ARTICLE INFO

Article history:

Received: 11 August 2013;

Received in revised form:

25 July 2014;

Accepted: 5 August 2014;

Keywords

Database Security,
Access Control Policy,
MAC, DAC,
RBAC.

ABSTRACT

Now a days Public and private organizations increase their database system requirement for day-to-day business. Hence database security becomes more crucial as the scale of database is growing. A signified approach for protecting information which enforcing access control policies based on subject and object and their characteristics. There are many security models for database systems. The database security systems have developed a number of different access control policies for assuring data confidentiality, integrity and availability. In this paper we survey the concepts under access control policies for database security. We review the key access control policies such as Mandatory Access Control policy(MAC), Discretionary Access Control Policy(DAC), and Role Based Access Control Policy(RBAC) and propose a concept on RBAC policy that is instead of access control through role assigned to the users, the users are assigned by some level of access control.

Introduction

Since organizations are implementing database systems for daily business and make decision, database security becomes more crucial. These functions are inventory management and budgeting, payroll, and various types of forecasting. If these important data will lose or misuse, then it will affect on user and application and also affect on entire organization[5]. A complete solution to data security must provide the following three requirements: 1) secrecy or confidentiality refers to the protection of data against unauthorized disclosure, 2) integrity refers to the prevention of unauthorized and improper data modification, and 3) availability refers to the prevention and recovery from hardware and software errors and from malicious data access denials making the database system unavailable. These three requirements arise practically in all application environments. Consider a database that stores payroll information. It is important that salaries of individual employee not be released to unauthorized users, that salaries be modified only by the users that are properly authorized, and that paychecks be printed on time at the end of the pay period. Similarly, consider the web site of an airline company. Here, it is important that customer reservations only be available to the customers they refer to, that reservations of a customer not be arbitrarily modified, and that information on flights and reservations always be available. In addition to these requirements, privacy requirements are of high. Though the term privacy is often used as a synonym for confidentiality, the two requirements are quite different. Techniques for information confidentiality may be used to implement privacy; however, assuring privacy requires additional techniques, such as mechanisms for obtaining and recording the consents of users. [1].

Data protection is ensured by different components of a database management system (DBMS). In particular, an access control mechanism ensures data confidentiality. Whenever a subject tries to access a data object, the access control mechanism checks the rights of the user against a set of authorizations, stated usually by some security administrator. An authorization states whether a subject can perform a particular action on an object. Authorizations are stated according to the access control policies of the organization.

Recently most relational database management systems (RDBMS) provide only some limited security techniques. They range from the simple password protection offered by Microsoft Access to the complex user/role structure supported by advanced relational databases like Oracle Server. There are some functional areas for database security models such as security policies, security mechanisms and security system assurance. Security policy describes what the security system is expected to do. Security mechanisms explain how the security systems should achieve the security goals. System assurance is used to provide consistency and integrity of the security mechanisms [8].

Access Control Policies

The policies through which the user access data object, called access control policies. In access control policies, access control mechanisms are used for securing databases. Whenever a user tries to access a data object, the access control mechanism checks the rights of the user against a set of fixed authorization. Basically there are two main access control policies, such as Mandatory Access Control policy and Discretionary Access Control Policy. Now a days another policy is used that is RBAC (Role Based Access Control) policy which is most popular access control policy and has been used for many applications, such as grid and multilevel database security system.

Mandatory Access Control(MAC) Policy

MAC policy is based on the classification of subject and object. Through this classification, this policy controls the access. The security levels of subjects and objects are classified into Top Secret(TS), Secret(S), Confidential(C), and Unclassified (U) in the relations such that TS>S>C>U. This access control policy defines two rules :

- A subject can read only objects in the equal or lower level than itself.
- A subject can read and write objects, that means record the objects when the level of subject is equal or higher than level of object.

Tele:
E-mail addresses: tarai.trilochan@gmail.com

This policy is usually applied to mass data which generally needs to be strong protection. MAC policy is well-known implemented in Multilevel Security(MLS), which traditionally has been available mainly on computer and software systems deployed at highly sensitive government organizations such as the intelligence community or the U.S. Department of defence[8].

Discretionary Access Control(DAC) Policy

DAC policy controls the data access according to the user's identification and authorization. These authorizations are known as rules. These rules specify the access modes for each users or group of users and each object in the system. This policy can be defined as a means of restricting access to objects according to the identity of subjects or groups to which they belong. This policy specifies the decision that who can access information at the discretion of the information creator. That means owner of data or database administrator. Implementation of Security policy is based on granting and revoking privileges. Access is granted or denied according to the identification o the user. The authorization administration policy supervises this function in DAC. There are two types of Common Administration Policies in DAC, such as Centralized Administration and Ownership Administration. In Centralized Administration, only some privileged subjects may grant and revoke authorizations while in Ownership Administration grant and revoke operations on data objects are entered by the creator(or owner) of the object. User-level privileges in DAC defines access permissions based on the general account information of user[1][8].

The flexibility of DAC policy make suitable for a variety of systems and applications. DAC policy have the drawback that they do not provide real assurance on the flow of information in a system.

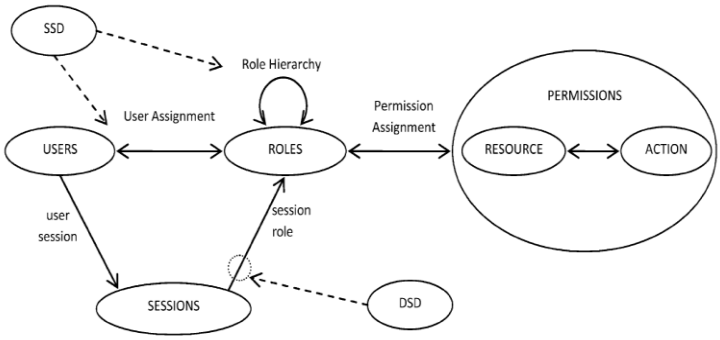
Role-Based Access Control Policy(RBAC)

This policy is one of the important policy which is recently innovated and widely used in organization. It direct represents access control policies of organizations and simplify authorization administration. Role based policies manage user's access to the information on the basis of the activities of the users. That means this policy is based according to the role of the users. A role is nothing but a specific function in an organization or some set of actions or responsibilities associated with this function. All authorization needed to perform a certain activity are granted to the role associated with that activity. The user access to object is regulated by roles. That means each user is authorized to play certain roles and on the basis of these roles, a user can perform access to the object. This policy consists two parts : one which assigns access rights for object to roles. This represent management of security. Another important point is suppose user responsibilities changed that means the user's current role can be taken away and new roles assigned as appropriate for the new responsibilities[3][4].

NIST RBAC Reference Model

In recent years, vendors have begun implementing role-based access control (RBAC) features in their database management, security management. Several RBAC models have been proposed without any attempt at standardizing salient RBAC features. For an individual user based on the role, the RBAC reference model takes the access decision. The access rights are grouped by role, and the access to a resource is granted only to users authorized to play the associated role. The NIST RBAC model defines four components : Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations(SISD), and Dynamic Separation of Duty Relations(DSD).

Core RBAC embodies the essential aspects of RBAC. There are five basic data elements of the Core RBAC component: Users, Roles, Resource, Permissions and Sessions. A *user* is defined as a human being. Although the concept of a user can be extended to include machines, networks, or intelligent automated agents, for simplicity reasons we limit a user to a person in this article. A *role* is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role. Permission is an approval to perform an operation on one or more RBAC protected objects. Session is the mapping between a user and a subset of roles enabled for the user. An operation is an executable image of a program, which upon invocation executes some function for the user. The types of operations and objects that RBAC controls are dependent on the type of system in which they will be implemented. For example, within a file system, operations might include read, write, and execute; within a database management system, operations might include insert, delete, append, and update. The basic concept of RBAC is that users are assigned to roles, permissions are assigned to roles, and users acquire permissions by being members of roles. Core RBAC includes requirements that user-role and permission role assignment can be many-to-many. Thus the same user can be assigned to many roles and a single role can have many users. Similarly, for permissions, a single permission can be assigned to many roles and a single role can be assigned to many permissions. Core RBAC includes requirements for user-role review whereby the roles assigned to a specific user can be determined as well as users assigned to a specific role. A similar requirement for permission-role review is imposed as an advanced review function. Core RBAC also includes the concept of user sessions, which allows selective activation and deactivation of roles. Finally, Core RBAC requires that users be able to simultaneously exercise permissions of multiple roles[2][7][9]. The following figure-1 represents the elements and relations specific to each component.



Hierarchical RBAC is the Core RBAC enhanced with the role hierarchy. It adds requirements for supporting role hierarchies. A hierarchy is mathematically a partial order defining a seniority relation between roles, whereby senior roles acquire the permissions of their juniors, and junior roles acquire the user membership of their seniors. They are many to many relations and define inheritance relations among roles that is role X inherits role Y if all permissions granted to role Y are also granted to role X.

Roles can have overlapping capabilities; that is, users belonging to different roles may be assigned common permissions. Furthermore, within many organizations there are a number of general permissions that are performed by a large number of users. As such, it would prove inefficient and administratively cumbersome to specify repeatedly their general

permission role assignments. To improve efficiency and support organizational structure, RBAC models as well as commercial implementations include the concept of role hierarchies. This constraint is inherited also within a role hierarchy.

Then the model component, Static Separation of Duty Relations, adds relations among roles with respect to user assignments. The constraints on the relations between elements take the form of Static Separation of Duty(SSD) relations and Dynamic Separation of Duty(DSD) relations. The SISD relation specifies the constraints on the assignment of users to roles. Once a role is authorized to a user, then the user can't be the member of a second role. DSD relations place constraints on the roles that can be activated in a user's session. If one role that takes part in a DSD relation is activated, the user cannot activate the related (conflicting) role in the same session[2][3].

From the above discussion we knew as per RBAC model, access rights are provided to group of users based on the role and governed by Dynamic Separation of Duty (DSD) relations. This model never described the category of roles under different levels of system i.e. level based role categories. In this paper we propose to assign different category of roles under some levels of a system with the concept in view that a particular level can be granted authorization up to a certain maximum level described by Database Administrator.

Comparative study of access control policies

	Mandatory Access Control Policy(MAC)	**Discretionary Access Control Policy**	**Role Based Access Control Policy**	**Level Wise Roll Based Access Control Policy(proposed)**
Access of information	Accessed by defining two rules	Through owner of information	By assigning roles	By assigning roles under some levels
Access Based on	Classification of subject and object	Human interpretation of good and bad user	Classification of roles	Classification of levels
Flexibility for accessing information	Low	High	High	Higher
Support for multilevel database system	Yes	No	Yes	Yes
Support for grid database system	No	No	Yes	Yes
data privacy	No	No	No ,but it occurs through some modifications	Yes

Proposed Model

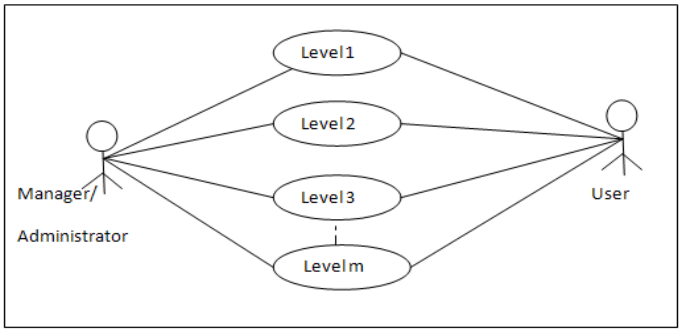


Figure 1

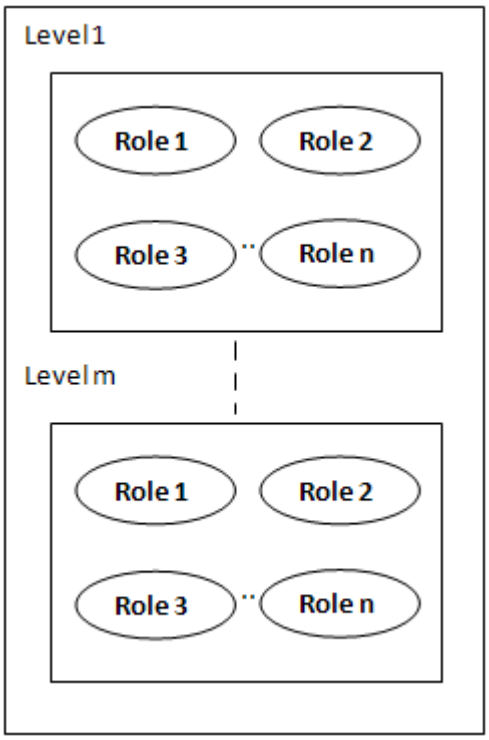


Figure 2

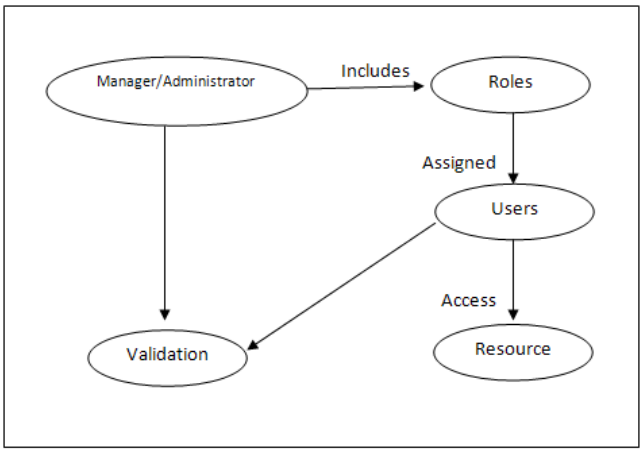


Figure 3

Figure-1 represents that the DBA creates different levels for users and will indicate that which user belongs to which level. After that figure-2 represents that role is assigned to the user that must under a level. In this way level and role is categorized. The figure-3 represents the mechanism of the modified RBAC policy(Level Wise Roll Based Access Control Policy). The mechanism is first the administrator assign the role to the user according to the level wise. Then the user is validated by the admin, then after validation the user will access the resource. Here in this policy, data privacy is maintaining. Because it is not possible that if a user of one level want to access the role assigned of another level.

Conclusion

Now a days the implementation of database systems are the key concept of data management for day-to-day operations of any organization. The scale of database is becoming larger and the user access control is complicated. So security of data management of system becomes crucial. So there are lots of requirements of access control mechanisms to achieve secrecy, integrity, and availability of data. In this paper we reviewed some access control models such as :Mandatory Access Control(MAC), Discretionary Access Control(DAC), and Role Based Access Control(RBAC) model. Especially we are

focusing RBAC model. In this paper we propose a policy that is Level Wise Roll Based Access Control Policy(LWRBAC) to assign different category of roles under some levels of a system with the concept in view that a particular level can be granted authorization up to a certain maximum level described by Database Administrator. The proposed policy represents that according to the level wise, the role is assigning to the user by administrator. If the user is valid, then the user will access the resource.

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, Vineela Muppavarapu 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.