Database Access Control Policies

Akshay Patil* and Prof. B. B. Meshram**

*(Department of Computer Technology, VeermataJijabai Technical Institute, Mumbai - 19)
**(Department of Computer Technology, VeermataJijabai Technical Institute, Mumbai - 19)

Abstract—As organizations increase their dependence on database systems for daily business, they become more vulnerable to security breaches even as they gain productivity and efficiency advantages. A truly comprehensive approach for data protection must include mechanisms for enforcing access control policies based on data contents, subject qualifications and characteristics. The database security community has developed a number of different techniques and approaches to assure data confidentiality, integrity, and availability. In this paper, we survey the most relevant concepts underlying the notion of access control policies for database security. We review the key access control models, namely, the discretionary and mandatory access control models and the role-based access control (RBAC) model.

Keywords— Database Security, Access Control Model, RBAC, DAC, MAC, Data Access Model

1. INTRODUCTION

As organizations increase their adoption of database systems for day-to-day operations and decision making, the security of data managed by these systems becomes crucial [1]. These functions include the various types of forecasting, payroll, inventory management and budgeting. Damage and misuse of such highly important data can affect not only a single user or application, but can also have disastrous consequences on the entire organization[1], [2]. The unauthorized disclosure, alteration or theft of an organization's information can have serious financial, legal, safety and privacy impacts on various stakeholders. Thus security is paramount to database administrators seeking to protect their vital business data from the prying eyes of unauthorized outsiders and insiders attempting to exceed their authority. The main goal of database security is *Information Security* during all database transactions[2]. Database Security can be defined as protecting information against unauthorized disclosure, alteration or destruction using hardware or software techniques. We can also define database security as the mechanisms that protect the databases against intentional or accidental threats. While designing such a system, trade-offs between operating environment, economic considerations and performance must be made[6].

Database security involves many issues such as legal and ethical issues regarding the right to access the private information. Unauthorized data observation results in disclosure of information to users not entitled to gain access to such information.Incorrect Data Modification, either intentional or unintentional result in an incorrect database state. Any use of incorrect data may result in heavy losses for organization[2], [6].

The complete solution to data security must meet the three main requirements of *Confidentiality*, *Integrity* and *Availability*. Confidentiality means protection of data against unauthorized disclosure. Prevention of unauthorized and improper data modification ensures Integrity of data. One can make sure that data is always available by prevention and recovery from hardware and software errors and from malicious data access denials. Figure 1 displays the concept of CIA triangle demonstrating the importance of major data security requirements. In addition to these basic requirements we also need to consider the Privacy requirements. Data privacy is required even after the disclosure of data. Data privacy implies that data should be used only for the purposes sanctioned by the owner to user and not misused for other purposes [2].

All database management systems provide some sort of intrinsic security mechanisms designed to minimize the threats. 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.The functional areas for database security model are *Security Policies*, *Security Mechanisms* and *Security System Assurance*. Security Policy describes what the security system is expected to do. Security Mechanisms explains how the security system should achieve the security goals. System assurance is used to provide consistency and integrity of the security mechanisms[8].

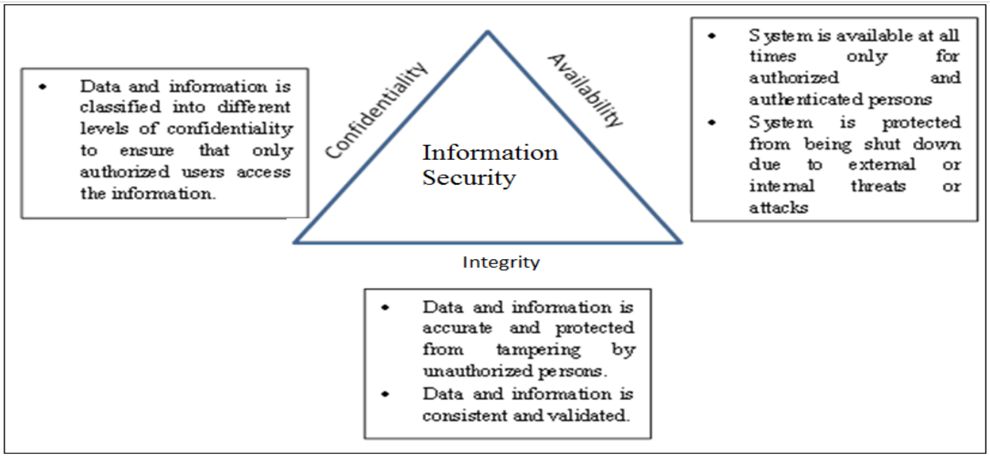
Data and information is classified into different levels of confidentiality to ensure that only authorized users access the information.
Confidentiality
Information Security
Availability
System is available at all times only for authorized and authenticated persons
System is protected from being shut down due to external or internal threats or attacks
Integrity
Data and information is accurate and protected from tampering by unauthorized persons.
Data and information is consistent and validated.

Figure 1: Information Security CIA Triangle[1]

2. ACCESS CONTROL POLICIES

Access Control Mechanisms are used for securing databases. It ensures data confidentiality. Whenever a user tries to access a data object, the access control mechanism checks the rights of the user against a set of fixed authorizations. Different policies can be combined to provide a more suitable protection to database system[4].

There are two main access control policies - *Mandatory Access Control Policy* and *Discretionary Access Control Policy*. In modern age new access control policy -*Role Base Access Control*is used. The RBCA is most popular access control model and has been used in various applications – e.g. in grid and multilevel databases Security System.

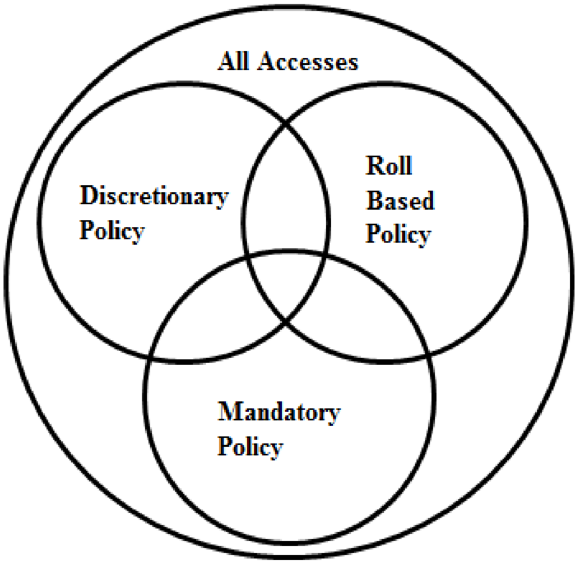

Figure 2: Different Access Control Policies[6]

3. DISCRETIONARY ACCESS CONTROL POLICY

Discretionary protection policies govern the access of users to the information on the basis of the user's identity and authorizations. These authorizations are also known as *rules*. These rules specifythe access modes, for each user (or group of users) and each object in the system. Discretionary Access Control (DAC) can be referred as a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. This policy places the decision of who can access information at the discretion of the information creator i.e. owner of data or database administrator. Security policy implementation is based on granting and revoking privileges. Access is granted or denied based on the identification of the user. The Authorization Administration Policy supervises this function in DAC. Common Administration Policies used in DAC are 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[6].User-level privileges in DAC defines access permissions based on the general account information of user, whereasthe relation-level privileges control access to the individual relations of the database[1], [6]. Figure 3 gives basic implementation of DAC.

The flexibility of discretionary policies makes them suitable for a variety of systems and applications. Discretionary access control policies have the drawback that they do not provide real assurance on the flow of information in a system.[7]

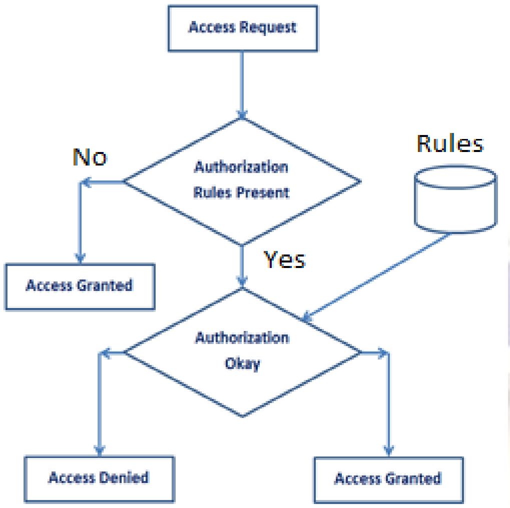

Figure 3: Discretionary Access Control Policy[1]

4. MANDATORY ACCESS CONTROL POLICY

Mandatory Access Control (MAC) constrains the ability of a subject (i.e. user) to access or generally perform some sort of operation on an object. MAC policy requires all users to follow the rules of access set up by the Database Administrator (DBA). This policy needs objects (e.g. Database) to be classified and subjects (e.g. Users, Process) to be cleared.It is enforced by comparing attributes of a subject and an object to control access to the object. It restricts access to objects based on the sensitivity of the information. It also provides an environment that restricts users to sharing information only within the same project, department or organization[1], [2], [5].Figure 4 gives basic concept of MAC Policy.

Access control in MAC model is based on the two principles, No read-up and No Write-down. In No Read-up, a subject can read only those objects whose access classes are dominated by the access class of the subject. In No Write-down, a subject can write only those objects whose access classes dominate the access class of the subject[6].

The enforcement of these principles prevents information in a sensitive object from flowing, through either read or write operations, into objects at lower or incomparable access classes. The introduction of such access control models requires addressing several issues.In the simplest case, the securitylevel is an element of a hierarchical ordered set.In most common arenas, thehierarchical set of security levels generally consists ofTop Secret (TS),Secret (S), Confidential (C), and Unclassified (U),where TS > S > C > U[6]. Each security level is saidto dominate itself and all others below it in thishierarchy.Access to an object by a subject is grantedonly if some relationship (depending on the typeof access) is satisfied between the securitieslevels associatedwith the two. A well-known implementation of MACis Multilevel Security (MLS), which, traditionally, hasbeen 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.

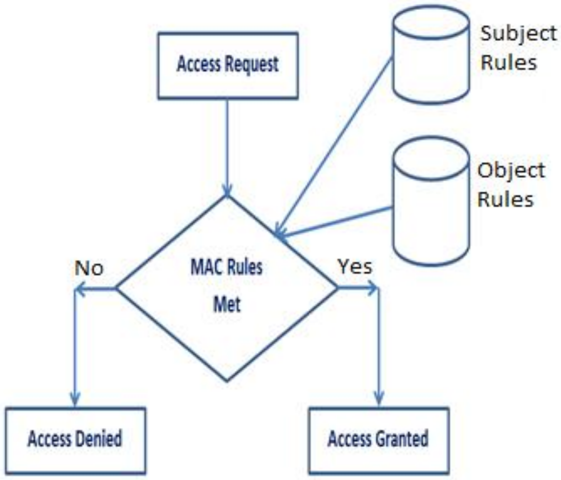

Figure 4: Mandatory Access Control Policy[1]

5. ROLE BASED ACCESS CONTROL POLICY

RoleBased Access Control (RBAC) models represent the most important recent innovation in access control models. RBAC has been motivated by the need to simplify authorization administration and to directly represent access control policies of organizations. Role-based policies regulate users' access tothe information on the basis of the activities the users execute in the system i.e. RBAC models are based on the notion of role.A *Role* represents a specific function within an organization and can be seen as a set of actions or responsibilities associated with this function.Under an RBAC model, all authorizations needed to perform a certain activity are granted to the role associated with that activity, rather than being granted directly to users. Users are then made members of roles, thereby acquiring the roles' authorizations. Thus user access to objects is mediated by roles; each user is authorized to play certain roles and, on the basis of these roles, a user can perform accesses to the objects[2], [7].

Authorization Management in RBAC

Role-based policiesbenefit from a logical independence in specifyinguser authorizations by breaking this task intotwo parts, one which assigns users to roles andone which assigns access rights for objects toroles. This simplifies security management.For instance, suppose auser responsibilities change, the user's current roles canbe taken away and new roles assigned as appropriatefor the new responsibilities. Since authorizations are not directly between users and objects, no revoke operation is required.

The RBAC Reference Model

The RBAC reference model takes the access decision for an individual user based on the roles the user has in the organization. The access rights are grouped by role name, and the access to a resource is granted only to users authorized to play the associated role. The NIST RBAC reference model (described in Figure 5) defines four model components: Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations (SSD), and Dynamic Separation of Duty Relations (DSD).The Core RBAC defines the minimum set of elements and relations that completely describe a role based access control system. There are five basic data elements of the Core RBAC component. Those are *Users* (i.e. Human beings or automated agents), *Roles* (i.e. Job functions or job titles which defines an authority level), *Resource* (i.e. Object which supports a set of possible Actions),*Permissions* (i.e. Approvals to perform an action on a given resource) and *Sessions* (i.e. mappings between a user and a subset of roles enabled for the user)[4].

The key concepts of RBAC are the many-to-many role relations: The user to role assignment (User Assignment) relations and the permission to role assignment (Permission Assignment) relations. The permissions associated to the roles are granted to the users only when the roles assigned to users are enabled.

The Hierarchical RBAC is the Core RBAC enhanced with the role hierarchy (Role Hierarchy) relations. They are many-to-many relations and define inheritance relations among roles that is, role A inherits role B if all permissions granted to role B are also granted to role A[3].

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 SSD relation specifies constraints on the assignment of users to roles. Thus if a user is authorized as a member of one role, the user is prohibited from being a member of a second role. This constraint is inherited also within a role hierarchy[3].

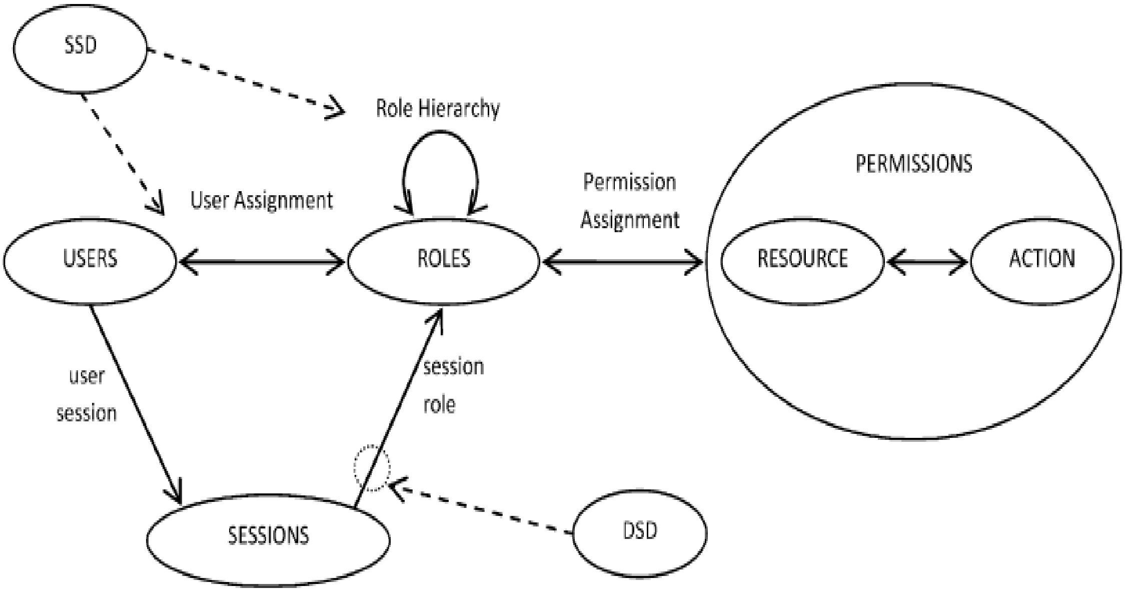

Figure 5: RBAC Reference Model[4]

Due to the distributed nature of GridDatabases presents different security needs and access policies. Open Grid Services Architecture- Data Access and Integration (OGSA-DAI) provides the first implementation for these needs, whichuses RBAC via a role-map file that maps individual Grid users to database roles[2], [4], [7].The ATLAS access control system in CERN Lab implements the Hierarchical RBAC model and allows for extensions with constraints to satisfy the experimental needs of accessing critical resources with many users with different security permissions[3]

DISCUSSION

	Discretionary Access Control Policy	**Mandatory Access Control Policy**	**Role Based Access Control Policy**
Access of information	Through Owner of Information	Through Fixed Rules for accessing information	Through Roles
Access Based on	Human Interpretation of good and bad user	Classification of users	Classification of Roles
Flexibility for accessing Information	High	Low	High
Access Revocation Complexity	Very Complex	Very Easy	Very Easy
Support for Multilevel Database System	No	Yes	Yes
Support for Grid Database System	No	No	Yes
Support for Hierarchical Database System	No	No	Yes
Consideration for Data Privacy requirement	No	No	No; but can be used with few modifications
Used in	Initial Unix System	The U.S.Department of Defence.	ATLAS experiment in CERN

6. CONCLUSION

The adoption of database systems as the key data management technology for day-to-day operations and decision making has overwhelmingly increased which makes the security of data managed by these systems becomes crucial. Access control mechanisms are required to achieve secrecy, integrity and availability of data. In this paper we have reviewed the two basic access control models (i.e. Discretionary and Mandatory Access Control Model) along with Role Based Access Control. The traditional models are no longer used as it is in complex database system due to their rigidness. The Role-Based-Access-Control (RBAC) model is very popular among current access control models as it simplifies the database access through notion of Role. It is widely used in different areas to provide efficient and flexible access to databases.

REFERENCES

[1] Feikis John, “Database Security”, IEEE Journals, February-March 1999

[2] Bertino Elisa and Sandhu Ravi, “Database Security—Concepts, Approaches, and Challenges”, IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 1, January-March 2005

[3] Marius ConstantinLeahu, Marc Dobson, and Giuseppe Avolio, “Access Control Design and Implementations in the ATLAS Experiment”, IEEE Transactions on Nuclear Science, Vol. 55, No. 1, February 2008

[4] 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

[5] Ravi S. Sandhu and PierangelaSamarati, “Access Controls Principles and Practice”, lEEE Communication\ Magazine September 1994

[6] Ravi S. Sandhu, Edward J. Cope , Hal L. Feinstein, , Charles E. Youman, “Roll Based Access Control Models”, IEEE Journals, February 1996