SURVEY OF ACCESS CONTROL TECHNIQUES USED IN DATABASE SECURITY

Shruti Adarsh

M.Tech Student, IT Department, IGDTUW, Delhi, India

Abstract

Data security concerns are increasing. In addition to the traditional requirements of data confidentiality, availability and integrity, new requirements are emerging such as data quality, completeness, timeliness, and provenance. Databases are the repositories of the most important and expensive information in the enterprise. With the increase in access to data stored in databases, the prevalence of attacks against those databases has also increased. Database security becomes more crucial as the scale of database for public and private organizations is growing and the various user access schemes are required. Recently, most relational database management systems (RDBMS) provide only some limited security techniques, which generally use a policy-based access control. A database system protects data from unauthorized access or modification through two aspects of function: data protection and access control. The data protection is achieved by data encryption, which is based on the techniques of Data Encryption Standard and the Public Key encryption. Access control is an important approach for protecting information privacy. It deals with the process of restricting access to data resources only to authorized subjects. In the fields of physical security and information security, access control is the selective restriction of access to a place or other resource. Due to various requirements for the user access control to large databases, security of databases has been emphasized. For this, various access control techniques have been proposed for database systems. The most popular access control policies currently used are Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC). In this survey paper, we will discuss about the access control techniques in relational database systems.

Key Words: *Database security, Access control, MAC, RBAC, DAC.*

----------***----------

1. INTRODUCTION

Databases are the repositories of the most important and expensive information in the enterprise.A database system protects data from unauthorized access or modification through two aspects of function: data protection and access control [1].The data protection is achieved by data encryption, which is based on the techniques of Data Encryption Standard and the Public Key encryption. Access control is an important approach for protecting information privacy. It deals with the process of restricting access to data resources only to authorized subjects.

Most relational database management systems (RDBMS) provide only some limited security techniques, which generally use a policy-based access control [2]. The most popular access control policies currently used are Mandatory Access Control(MAC),Discretionary Access Control(DAC), Role-Based Access Control(RBAC) [3].

1.1. MAC Policy

Mandatory Access Control (MAC) policy is based on a security model designed by Bell and LaPadula for an operating system. This policy regulates the access according to the classification of subjects and objects in a system. The security levels of subjects and objects are classified into Top-secret(TS), Secret(S),Confidential(C), and Unclassified(U) in the relation of TS > S > C > U[4]. This policy defines two basic rules: a subject can read only objects in the equal or lower levels than itself, and a subject can record only objects in the equal or higher levels than itself. This policy is usually applied to mass data, which generally needs to be strongly protected. However, the data integrity cannot be maintained because a lower level user possibly write on the higher level objects.

1.2. DAC Policy

Discretionary access control (DAC) policy is based on restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission on to any other subject [4]. Owing to the flexibility of this policy, most of previous DBMSs adopt it. However, the access right can be transferred to other users avoiding the data owner's recognition.

1.3. RBAC Policy

Role Based Access Control (RBAC) policy represent arguably the most important recent innovation in access control models. RBAC policy is based on the notion of role [4].

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 this policy, all authorizations needed to perform a given 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 possessing the roles' authorizations. User access to objects is interposed by roles; each user is authorized to play certain roles and, on the basis of the roles, he can perform accesses to the objects. Because a role groups a number of related authorizations, authorization management is greatly simplified. Whenever a user needs to perform a certain activity, the user only needs to be granted the authorization of playing the appropriate role, rather than being directly assigned the required authorizations. Also, when a user changes his function within the organization, one only needs to revoke from the user the permission to play the role associated with the function. This policy makes it possible to simplify the security management and to prevent the abuse of rights by allowing only least privilege to users.

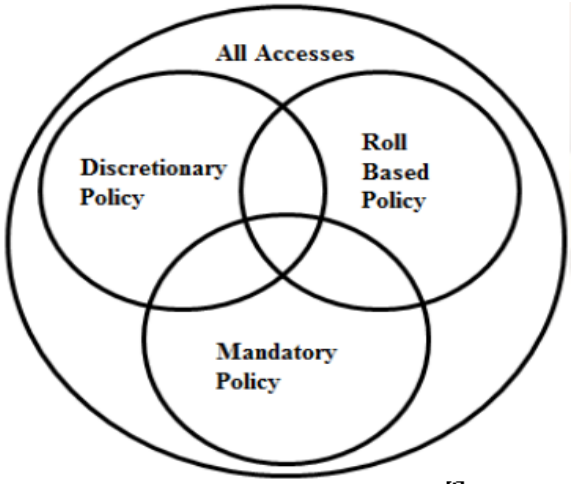

Fig-1: Different Access Control Policies [3]

2. RELATED WORK

There are various access control techniques based on the above policies.

A. Min-A Jeong et al. [5] proposed a database security system that can individually control user access to data groups of various sizes and is suitable for the situation where the user's access privilege to arbitrary data is changed frequently.

Authors have defined data group(s) in different sizes d, by the table name(s), attribute(s) and/or record key(s), and the access privilege is defined by security levels, roles and polices. They have also defined the user groups that can be characterized by security levels, roles or any partitions of users. The policies were represented in the form of Block(s, d, r) and were used to control access to any data or data group(s) that is not permitted in 'read' mode.

Methodology:

The proposed system operates in two phases. The first phase is of a modified MAC model and RBAC model. A user can access any data that has lower or equal security levels, and that is accessible by the roles to which the user is assigned. All types of access mode are controlled in this phase. In the second phase, a modified DAC model is applied to re-control the 'read' mode by filtering out the non-accessible data from the result obtained at the first phase. With this proposed security system, more complicated 'read' access to various data sizes for individual users can be flexibly controlled, while other access mode can be controlled as usual.

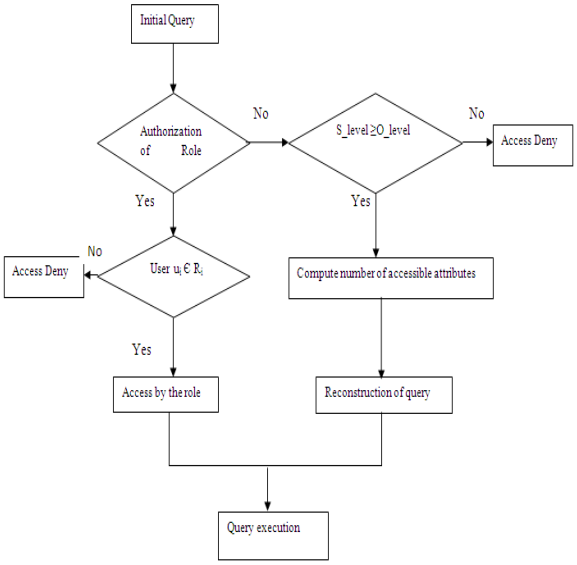

Fig-2: Diagram for the operational flow of the MAC and RBAC module [5].

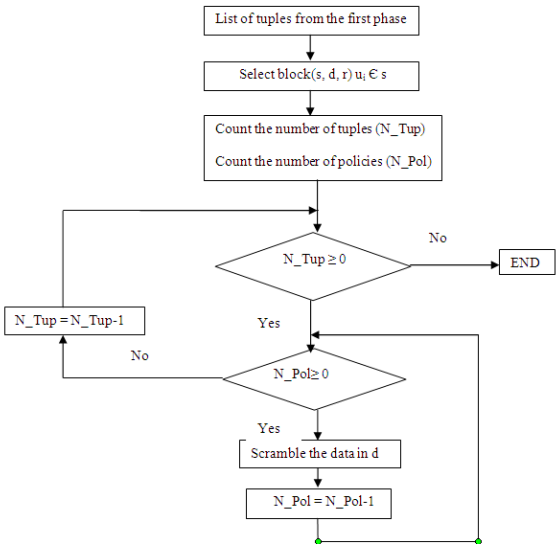

Fig-3: Flow diagram of S-DAC module [5]

Comments:

This database security system can individually control user access to data groups of various sizes and is suitable for the situation where the user's access privilege to arbitrary data is changed frequently.

B. Leon Pan [6] proposed a criterion-based access control approach to deal with multilevel database security. This approach was first proposed to integrate with role-based access control but it also worked well independently.

Methodology:

In this approach, authorization rules were transformed to security criteria, security criterion expressions, and security criterion subsets.
Security criterion is used to specify the user's security attributes and define object's security attributes. Security criterion expression is a Boolean Expression in terms of security criteria. Security criterion subset is used to specify user's security attributes, which usually depends on user's position and job responsibility. The logical structure of the criterion-based access control approach achieves the goal of database security by using security mechanism between users and the database. The security mechanism plays the role of collecting users' security attributes and of filtering the information according to them. When a user requests for access, security mechanism decides whether the user has access to the wanted object or not.

The security criterion expressions embedded in a secure object serve as locks, while security criteria in security criterion subset serve as keys. When a secure user accesses a secure object, he uses the available keys to move the locks. The security criterion expressions are evaluated in two steps. First by substituting all the security criteria in security criterion expression with true T or false F, following the rule: all security criteria in a security criterion expression which also appears in secure user's security criterion subset should be set value true T, while other have value false F. The second rule is that security criterion expression is evaluated according to the normal evaluation procedure in Boolean algebra. Value T implies users with these security criteria are not allowed to access the corresponding secure sub object whereas value F implies that the security criterion expression does not prevent these secure users from accessing the object. The fine-grained access is achieved by evaluating every associated security criterion expression with the security criteria in related secure user's security criterion subset.

Table – 1: A secure object of customer table [6]

F	F	F	$s_1 \wedge s_2$	$(s_1 \wedge s_2) \vee (s_1 \wedge s_2)$
Name	Address	Inv.	Mortgage	F
A	PQR	10000	6579	F
B	XYZ	3434	7896	$s_1 \wedge s_2$
C	UVW	3344	6435	F
-	-	-	-	-
E	GHI	3545	7899	$s_1 \wedge s_2$
F	HIK	5457	1000	F

Comments:

This approach of applying the criterion-based access control to deal with multilevel database access control is novel in nature and it does not increase the storage cost also because only one row and one column is added only in the table. Efficiency of the system can be improved by first evaluating the logical "OR" of the different security criterion expressions.

C. Ying-Guang Sun [7] proposed an access control method for distributed database system. The method is based on multi-level security tag and mandatory access control policy. The author in his paper designed Multi-level security system structure and defined the security tags of subjects and objects. Mandatory access control was achieved by modifying the user's query statement and using security tag table in distributed database system.

Methodology:

He used the concept of Bell-LaPadula Model to introduce the concepts such as subject, object and domain. He also presented the concept of security tag and security tag table. Every security tag is defined as (Scope, S-Level), Scope represents the domain or the object, which is not classified by size ;S-Level represents security level ,for example, top secret, secret, confidential, general. The safety tag of subject is expressed as :(Scope-S, S-Level-S). The security tag of object is expressed as :(Scope-O, S-Level-O). The security policy is defined as:
1) If and only if the security tag of object is equal to or less than the safety tag of the subject, i.e. ,S-Level-O≤ S-Level-S and the (Scope-O,S-Level-O)≤ (Scope-S,S-Level-S),the subject can read objects.
2) If and only if the security tag of object is equal to the safety tag of the subject, that is S-Level-O=S-Level-S and the Scope-O=Scope-S (denoted as (Scope-O, S-Level-O) = (Scope-S, S-Level-S)), the subject can modify object.

The structure of multi-level security system has three modules: security tag definition module, mandatory access control module and output check module.
The security tag definitions module completes security tag definition of subject and object for the database administrator, and it also carries out integrity and consistency checks on the subject and the object. The

mandatory access control module achieves security access control by modifying the query statement which the user submits. First, this module confirms the user's security tag. Then, according to the system security policies and the predefined data security tags, this module modifies the user's query statement from the local and global and submits them to the local DBMS. Output check Module checks the query results before the query results are returned to the user.

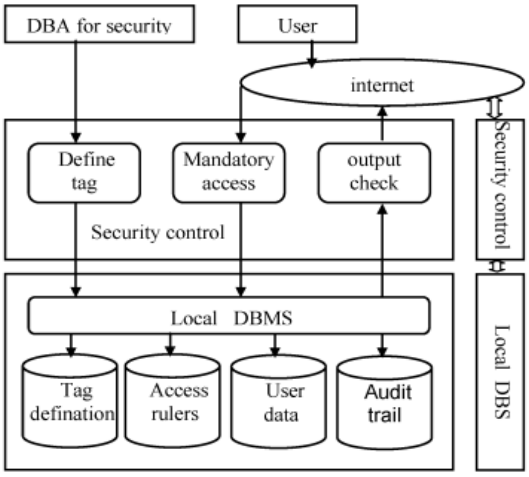

Fig-4: Multi-level security system structure for distributed database [7]

Comments:

To solve the problem of unsafe information flow and leakage of unauthorized information during data sharing, the security tags of subject and object are defined respectively, a mandatory access control policy is used and the flow path of information is controlled.

D. Trilochan Tarai et al.[8] proposed 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.

Methodology:

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 incorporate the essential aspects of RBAC. There are five basic data elements of the Core RBAC component: Users, Roles, Resource, Permissions and Sessions. Hierarchical RBAC is the Core RBAC enhanced with the role hierarchy. Static Separation of Duty Relations, adds relations among roles with respect to user assignments. The SISD relation specifies the constraints on the assignment of users to roles. DSD relations place constraints on the roles that can be activated in a user's session.

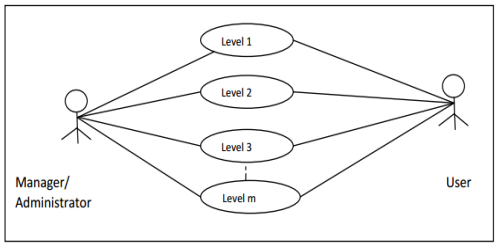

Fig-5: Diagram for different levels of users [8]

The above figure represents that the DBA creates different levels for users and will indicate that which user belongs to which level. After that figure- 6 represents the role assigned to the user that lies under a level. In this way level and role is categorized. The figure-7 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 maintained, because it is not possible that a user of one level access the role assigned of another level.

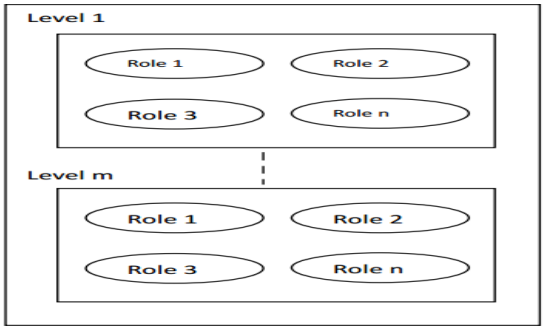

Fig-6: Roles assigned to users according to levels[8]

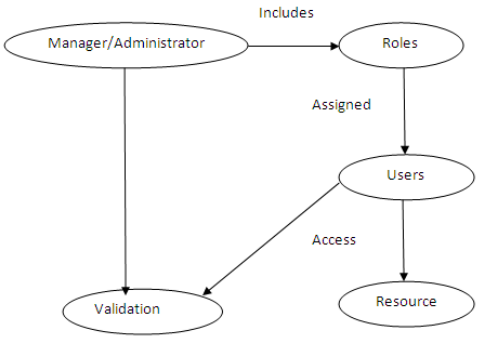

Fig-7: Level Wise Roll Based Access Control[8]

Comments:

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 is

proposed. The policy represents that the role is assigned to the user by administrator, level wise. If the user is valid, then the user will access the resource.

3. FUTURE SCOPE

Addressing network security and database security simultaneously leads to efficient unified security system. The information used for authentication can be reused for the preliminary access control and fine-grained access control. The termination of the users' requests at the early stage avoids processing the requests further unnecessarily. This kind of model can be applied to many areas such as finance, health care, government, and military.

4. CONCLUSIONS

As a lot of effort have been done to solve the issues of access control in database security, still there are some issues that needs to considered like the increase in overhead which may degrade the system performance. Also, there is a possibility that a new policy can be a duplication of existing policies. Therefore, a policy reduction methodology should be considered.

REFERENCES

[1] Nedhal A. Al-Sayid and Dana Aldlaeen "Database Security Threats: A Survey Study," 5th International Conference on Computer Science and Information Technology (CSIT) in 2013.

[2] Sohail Imran and Dr. Irfan Hyder "Security Issues in Databases" Second International Conference on Future Information Technology and Management Engineering 2009.

[3] Akshay Patil, Prof. B. B. Meshram "Database Access Control Policies"International Journal of Engineering Research and Applications (IJERA),Vol. 2, Issue 3, pp.3150-3154, May-Jun 2012.

[4] Elisa Bertino and Ravi Sandhu, "Database Security—Concepts, Approaches, and Challenges" IEEE Transactions on dependable and secure computing, Vol. 2, No. 1, January-March 2005.

[5] Min-A Jeong, Jung-Ja Kim and Yonggwan Won "A Flexible Database Security System using Multiple Access Control Policies", pp 236-240, IEEE 2003.

[6] Leon Pan "Using Criterion-Based Access Control for Multilevel Database Security" International Symposium on Electronic Commerce and Security, pp 518-522, IEEE 2008.

[7] Ying-Guang Sun "Access Control Method Based on Multi-level Security Tag for Distributed Database System" International Conference on Electronic & Mechanical Engineering and Information Technology, pp 2509-2512, IEEE 2011.

[8] T. Tarai and Pradipta Kumar Mishra "Enhancing database access control policies" American International Journal of Research in Science, Technology, Engineering & Mathematics, 3(1), pp. 109-113, June-August, 2013.

BIOGRAPHIES

Shruti Adarsh is pursuing her M.Tech(final year) in Information Security Management from Indira Gandhi Delhi Technical Univrsity,Kashmere Gate,Delhi and has done her B.Tech from ABES Institute of Technology,Ghaziabad.