Database Security Model using Access Control Mechanism in Student Data Management

Aye Mon Win, Khin Lay Myint

Faculty of Information Science, University of Computer Studies, Hinthada, Myanmar

ABSTRACT

Database security means the protection of data against unauthorized disclosure, alteration, destruction. This paper present a procedure to implement a Data Access Policy to ensure the protection of privacy rights of students' records within student data management system. According to the system, the administration of different security levels, resources, users, tasks etc. is indispensable. This paper focused on a student data management system by using Data Access Control model. According to the concept, only the administrator has the privilege to manage or administer the data. She/he provides all types of privileges required to maintain users, their authorization and access, and the authorized resources. The administrator controls the largest information. This system we present DAC access control mechanism using MySQL database.

KEYWORDS: *database security, access control, roles, privileges, authorization*

How to cite this paper: Aye Mon Win | Khin Lay Myint "Database Security Model using Access Control Mechanism in Student Data Management" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-3, April 2019, pp.529-531, URL: http://www.ijtsrd.com/papers/ijtsrd22820.pdf

IJTSRD22820

INTRODUCTION

Today all organizations rely on database systems as the key data management technology for a large variety of tasks, ranging from day-to-day operations to critical decision making. Such widespread use of database systems implies that security breaches to these systems affect not only a single user or application, but also may have disastrous consequences on the entire organization. Any information management needs to protect their resources, and data against such an unauthorized revelation at the same time ensuring their accessibility to potential work use. Access control policy is one of the most popular and security mechanism.

During the daily work of administrative support for students' data, it was noticed that the ad-hoc requests for data access is resulting an inefficient use of time and resources. For example, for accurate and efficient of students' information, teachers' information and university related information as well as a student, need to get spontaneous up to date answers to different types of queries. Answers are needed quickly and efficiently taking into consideration all privacy and security requirements.

In a student data management environment, Data types are identified according to their nature and field, for example Academic Data, Personal Student Data, Administrative Data, Financial Data, Research and Development Data, HR Data. Each type of data or part thereof can be assigned a security attribute, such as Restricted, Limited Access, or Public, based on the level of its sensitivity and protection.

A. Access Control Model

The security mechanism of a DBMS must include provisions for restricting access to the database as a whole. This function is called access control. Access control is a core concept in security. The primary method used to protect data is limiting access to the data. This can be done through authentication, authorization, and access control. These three mechanisms are distinctly different but usually used in combination with a focus on access control for granularity in assigning rights to specific objects and users. For instance, most database systems use some form of authentication, such as username and password, to restrict access to the system. Further, most users are authorized or assigned defined privileges to specific resources. Access control further refines the process by assigning rights and privileges to specific data objects and data sets. In database security, objects contain to data objects such as tables, rows and columns as well as SQL objects such as views and stored procedures. Data actions include read (select), insert, update, and delete or execute for stored procedures.

For instance, Student A may be given login rights to the University database with authorization privileges of a student user which include read-only privileges for the Course_ Listing data table. Through this granular level of access control, students may be given the ability to browse course offerings but not to peruse grades assigned to their classmates. Limiting access to database objects can be demonstrated through the Grant/Revoke access control mechanism. Generally, access control is defined in three ways: Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role Based Access Control (RBAC).

I. Discretionary access control (DAC)

Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined byan object's owner group and/or subjects. DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password. DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users. In other words, the owner determines object access privileges.

II. Mandatory access control (MAC)

This policy allows a data user to access a certain data item only when his authority level matches the security level of the data item. MAC was mainly used and implemented in the military environments. The most common model of MAC is the multilevel security policy where access from subjects to objects is based on classes or clearance levels assigned to subjects and labels assigned to Objects

III. Role-based access control (RBAC)

Role-based-access-control (RBAC) is a policy neutral access control mechanism defined around roles and privileges. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments. RBAC can be used to facilitate administration of security in large organizations with hundreds of users and thousands of permissions. Although RBAC is different from MAC and DAC access control frameworks, it can enforce these policies without any complication.

B. Users and Roles as used in access control

In the student data management system, users are granted membership into roles based on their qualifications and responsibilities in the organization. The activities that a user is authorized to perform are usually based on the use's role. The User Membership into role(s) can be revoked and new memberships established especially when new operations are operated, and old activities can be deleted as the duties and organizational functions changes and evolves in the system. Therefore, administration and management of privileges are simplified in the process, roles can be updated without the privileges for every user on an individual basis. When a role is assigned to a User the user can be given no more privilege than is necessary to perform the job. This access control concept of least privilege needs, identifying the user's activity functions, which determines the least set of privileges needed to perform that function, and restricting the user to a domain where those privileges are. The access control policy is a very important aspect of database systems.

C. Functions of student data management environment

In the student data management environment, users belonging to different access right might need to perform common activities. Some general operations might be performed by all students. For example, user student can retrieve their records. In this paper the following functions are defined in relation to the student data management environment:

An administrator roles: These role includes multiple function, within the administrator one can define first the name and user's types, second assign privileges to users. He can assign a permission to a user, and authorizes or defines a password for users.

The head of department roles: In this model, the administrator give to the head of department all privileges of the access right.

A professor roles: In this system, an administrator give to a professor all permission of student performance information. He can give all or restrict access right to lecturer or can revoke his permission.

The clerk role: In the student data management system, the head of department give to the clerk insert permission. He has for privilege to register a new student. He has to fill the information such as name, DOB, Father Name, age, gender, etc.… according to the role.

A student role:
He or She can read only his/ her students records and cannot other access to the records.

User roles and permissions
are enforcing security in the system, access control policies define the user's rights on objects. It also defines the identification and authentication of each role. In this model, policies define which permissions are established to roles figure 1 in the student data management.

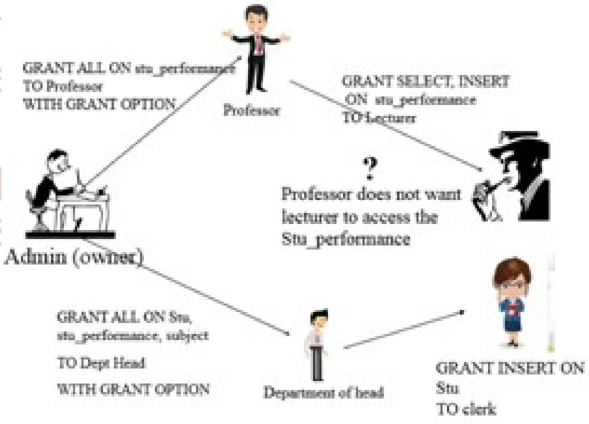

Figure.1. access control for authorized user

D. Database for Student data environment

In student data management system, all the students information stored in the database system. The data must only be accessed by the users who are defined or authorized. This is the first step for any information stored and any secure data. The following sample tables are stored in student_info database.

TABLE I: Student table

Sid	Sname	Age	City
1	Smith	20	Yangon
2	Adam	18	Yangon
3	Bob	21	Mandalay
4	Sue	20	Mandalay
5	Cathy	22	Hinthata

TABLE II: Subject table

S_code	Name
CST-201	Java
CST-202	Mathematics
CST-203	Digital Fundamentals
CST-204	Database System
CS-206	Software Engineering

TABLE III: Stu_performance table

Sid	S_code	Category
1	CST-201	Good
1	CST-202	Excellent
1	CST-203	Good
1	CST-204	Good
1	CS-206	Good
2	CST-203	Poor
2	CST-204	good

E. Acess control Grant and Revok

In the database security model, the ability to grant authorization to perform actions on objects resides with the authorize user of the object. A security policy specifies who is authorized to do what and based on the privileges for objects and views.

AUTHORIZE IN SQL: THE GRANT COMMAND. If a user has a privilege with the GRANT OPTION, can pass privilege on to other users with or without passing on the GRANT OPTION
Syntax: GRANT privileges ON object TO users [WITH GRANT OPTION]
Privileges of authorized persons:
For head of department: create user 'department head'@'locaclhost' identified by 'secure1';
Grant all on student_info.* to 'department head' with grant option;
For professor: create user 'professor'@'locaclhost' identified by 'secure2';
Grant all on student_info. stu_performance to 'professor' with grant option;
For lecturer: create user 'lecturer'@'locaclhost' identified by 'secure3';
Grant select, insert on student_info. stu_performance to 'lecturer';
For clerk: create user 'clerk'@'locaclhost' identified by 'secure4';
Grant insert on student_info.student to 'clerk';
Check the user professor is update permission,
ERROR 1142(42000): UPDATE command denied to user 'professor' @ 'localhost' for table stu_performance.
REVOKE privileges from lecturer:
REVOKE all on student_info form 'lecturer' @ 'localhost';
In student data management of database security system, grant command is used to provide access on the student database objects to the different users. The revoke removes user access rights to the database object.

F. Conclusion

Database security is an important goal of any data management system. Database security is based on three important constructs confidentiality, integrity and availability. Access control maintains a separation between users on one hand and various data and computing resources on the other. In student data management environment have unique specific security and privacy requirements. If management would like to apply access control mechanism in this information system to reduce the administrative tasks and manage the smooth running of the student performance, then several context awareness, strong personalization of access control policies that is efficient, flexible and fairly generic must be adopted. 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 Role. It is widely used in different areas to provide efficient and flexible access to databases.

G. References

[1] https://en.wikipedia.org/wiki/Access_control

[2] https://searchsecurity.techtarget.com/definition/access-control

[3] Surajit Chaudhuri, Raghav Kaushik, Ravi Ramamurthy "Database Access Control & Privacy: Is There A Common Ground?"

[4] Meg Coffin Murray -Kennesaw State University, Kennesaw, GA, USA "Database Security: What Students Need to Know".

[5] "KalpeshV.Chaudri A Survey on Secure Access Control Mechanism of Geospatial Data".

[6] Tresa F Lunt "Access Control Policies"

[7] Akshay Patil* and Prof. B. B. Meshram "Database Access Control Policies"

[8] Kriti, Indu Kashyap "Database Security & Access Control Models: A Brief Overview"

[9] cj date "Introduction to database system".

[10] Ji-Young Lim, Woo-Cheol Kim, Hongchan Roh, Sanghyun Park "A Practical Database Security Model Using Purpose-Based Database Access Control and Group Concept".

[11] Gregory Saunders1, Michael Hitchens2, and Vijay Varadharajan2 "Role-Based Access Control and the Access Control Matrix".

[12] Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE "Database Security—Concepts,Approaches, and Challenges?"

[13] Avik Chaudhuri "Foundations of Access Control for Secure Storage"

[14] Pierangela Samarati1 and Sabrina De Capitani di Vimercati2 "Access Control: Policies, Models, and Mechanisms"

[15] Chia-Chu Chiang and Coskun Bayrak "Modeling Role-Based Access Control Using a Relational Database Tool"