Database Security And Control Methods

Davinder Kaur
Dept of Computer Applications
Chandigarh Group of Colleges, Landran

Abstract- *This review paper focuses on data which is generated quickly and the destination of such data is database. The data is stored in database which is easy and well organized to manage the data. The operations such as data manipulation and maintenance are done using Database Management System. The importance of data in organization which is important to secure the data available in the database. An invulnerable database is the one which is retaliated from different possible database threats. The models are made for databases which are known as Security models. These models are different in many ways as they are dealing with different matters of the database security. They may different also because of they are taking different inference about what comprise a secure database. So, it becomes very tough for database security seekers to select suitable model for securing their database. This paper will discuss some of the attacks that can be possible with its counter measures and its control methods that can be possible. Securing database is important approach for the planning of directive based database security requirements. Ensuring security for database is very unfavorable issues for the companies. As complexity of database increases, it tend to have more complex security issues of database.*

Keywords- Security, database, control methods, integrity.

I. INTRODUCTION

A database is simply an organized collection of related data, typically saved on computer system's hard disk and accessible by many concurrent users. The users can enter and analyze the data quickly and easily. The data stored in the database are organized to process the information storage and retrieval. Databases are generally separated into application areas. For example, one database may contain human resource (employee and payroll) data, other may contain sales data, and another may contain accounting data and so on. The data are stored in many blocks in repository called database. The database which is user interface is known as database management system (DBMS). A Database Management System (DBMS) is the application software which interacts with the authorized user for creating and managing databases.

Data is a valuable resource for an organization and therefore should be kept secure and confidential. The database security is a crucial issue in the database management. The term "security" refers to the protection of the database against any unauthorized access that may be either intentional or accidental. Security in a database involves both policies and mechanisms that protect data from any unauthorized access.

Most of the database management systems are operated by multiple concurrent users. Some of them may be adding some new information and some of them may be deleting the existing information. Access by an unauthorized user might corrupt the database and make the database incorrect. Integrity implies that any unauthorized access, updation, or deletion of data in the database doesn't change the validity of the data. In other words, integrity ensures that changes made to the database by unauthorized users don't result in loss of data consistency.

II. SECURITY AND INTEGRITY THREATS

A threat is any situation, event or personnel which will adversely affect the database security and smooth and efficient functioning of the organization. Threat to database can be intentional or accidental. People can exploit loopholes or abuse privileges to intentionally or maliciously gain access to the confidential data. Following are the some database security threats:-

- **Data Tempering**- Confidentially and Integrity of information during transmission is essential and vital. Distributed environment brings the possibility that an unauthorized third party can perform a computer crime by tampering with data as it moves between sites. In a data modification attack, an unauthorized party on the network intercepts data in transit and modifies parts of that data before retransmitting it.

- **Eavesdropping and data theft**- Data must be stored and transmitted securely over the internet and in WAN's environment. Both public carriers and private network owners often root portions of their network through self-doubting landlines, particularly vulnerable satellites links or a number of servers.

- **Password related threats**- In large systems; user must remember multiple passwords for different services that they are entitled to use. Users typically respond to the problem of managing multiple

passwords by selecting simple to guess passwords such as name, a fictional character or a word found in a dictionary. Users choose the standardized passwords so that they are the same on all machines or websites and sometimes goto the extent of writing them down where an attacker can easily find them.

- **Unauthorized access to data**- Database may contain confidential tables or confidential columns in a table which should not be available indiscriminately to all users who are authorized to access the database. It should be possible to protect data on a column level; similarly, certain data rows may contain confidential information which should not be available indiscriminately to users who are authorized to access the table.

- **Lack of accountability**- There must be some reliable way to monitor users. In large scale environments, the burden of managing user accounts and passwords makes the system vulnerable to errors and attacks. Appropriate logs must enable to monitor accountability. These problems become particularly complex in a multitier system.

III. PRIVILEGES

A privilege is a right to execute a named object (i.e. database tables, views, procedures, triggers) in a prescribed manner. For example- A permission to create a table, right to select rows from another user's table, right to connect to the database (creating a session), permission to query a table etc.
A privilege can be granted to the user in the following two ways.

1. Explicitly by giving the right to the user to insert records into the table.
2. By granting privileges to the roles (which are basically a named group of privileges) and then granting roles to the user.

There are two distinct categories of privileges:-

a) System Privileges
b) Object Privileges

System Privilege: A system privilege is also known as account level privilege in which the DBA specifies the particular privileges that each account holds independently of the tables in the database. In other words, a system privilege is a right to perform a particular action, or to perform a particular action on a particular type of object. The examples of system privileges are

- Create table, Session.
- Create View
- Alter any procedure, role
- Drop privileges

The system privileges can be granted/revoked to users in Oracle using GRANT and REVOKE statements. Users who are granted system privileges using WITH ADMIN option can grant or revoke system privileges.

Object Privilege: An object privilege is also known as table level privilege which is used to access each individual relation, view, procedure, sequence, function etc, n the database. In other words, object level privileges are those guaranteed from a user to access or manipulate database objects. For example- A database user who wants to insert a row into the employee table of user must have granted a specific privilege to do this. Some of the object privileges are as follow:-

- Select applies to tables, views, sequences.

This privilege allows a user to issue a query against a table or view or select a value from a sequence.

- Insert, update and delete- All these apply to tables and views. These privileges enable the user to insert new rows, delete existing rows, and update existing rows in a table r view.
- Execute applies to procedures, functions and packages etc.
- References apply only to tables.

IV. CONTROL METHODS FOR DATABASE THREATS

Every organization must consist a security policy which should remove the threats. Authentication plays a very important role in security policy because there will be less chances of threats if there is proper authentication.

There are three security concerns of database. They are-

1. Confidentiality
2. Integrity
3. Availability

Confidentiality: - It means data is available to authorized subjects only. Confidentiality is equivalent to privacy. It ensures that sensitive information must not reach to wrong people, whereas right people can get the information.

Integrity: - It means that data can be modified by authorized users. It involves the accuracy, consistency and trustworthiness of data over its entire life span. There must be some steps to ensure that unauthorized users cannot alter the data.

Availability: - It means that whenever data is needed, it will be available. It is highly ensured by maintaining all the hardware.

V. CONCLUSION

There are many factors such as security concern progression, new computing paradigms and applications and the disinter conciliation of new access in which to apply the broaden approaches to accomplish the data security. There are many techniques to improve the security of database. In this paper, the information on different threats and security issues are discussed.

REFERENCES

[1] Ayyub Ali , Dr.Mohammad Mazhar Afzal, "Database Security: Threats and Solutions" International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 6, Issue 2 [Feb. 2017] PP: 25-27

[2] Mubina Malik and Trisha Patel "DATABASE SECURITY - ATTACKS AND CONTROL METHODS" International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016

[3] Elisa Bertino, Sushil Jajodia, Pierangela Samarati "Database security: Research and practice" Information Systems Volume 20, Issue 7, November 1995, Pages 537-556

[4] Sukhdev Singh Ghuman," Database Security", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 2, Issue. 2, February 2013, pg.102 – 105