www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -02 February, 2016 Page No. 15801-15804

Protecting the Database against Misuse

Kanika Sluja[1], Satinder Kaur[2], Mandeep Kaur[3]

[1]Post Graduate Department of Computer Science and Applications,

GHG Khalsa college, Gurusar Sadhar (Distt. Ludhiana)

kanikasluja@gmail.com

[2]Post Graduate Department of Computer Science and Applications,

GHG Khalsa college, Gurusar Sadhar (Distt. Ludhiana)

sat_grewal85@yahoo.com

[3]Post Graduate Department of Computer Science and Applications,

GHG Khalsa college, Gurusar Sadhar (Distt. Ludhiana)

mandy_pandher@yahoo.com

Abstract: **In the contemporary era, Data is the most valuable resource that is used in day to day life from an individual to large organizations. Database contains useful and confidential information so it becomes necessary to protect it from any unauthorized access. Any unauthorized user can try to perform unauthorized activities at unauthorized time on sensitive data. So to prevent the database from any misuse, different security mechanisms are applied to the database to make it secure. This paper focuses on the challenges and security mechanisms in database.**

***Index Terms*– data confidentiality, data privacy, database security, integrity.**

I. INTRODUCTION

Data or information is one of the most valuable assets in any firm. Almost all organizations are using computerized information systems. As database contains the vital information so it is highly maintained by the organizations. So database protection and security is a serious mechanism which protects the confidential data that is stored in a database.

Thus, a complete solution to data security must meet the following three requirements:

- Secrecy or confidentiality refers to the protection of data against unauthorized disclosure.
- Integrity refers to the prevention of unauthorized and improper data modification.
- Availability refers to the prevention and recovery from hardware and software errors and from malicious access denials making the database system unavailable.

At any level database security mechanisms can deal with any kind of illegal access to database to make it secure. Database security also faces difficulty while permitting or prohibiting user actions on the database and the objects inside it. Confidentiality is the main challenge for organizations that are running successfully of their databases. So that unauthorized user can not access their data and information. Assurance should also be there, that their data is secure against any malicious or accidental modification. Data protection and confidentiality are the security concerns.

Database security term means Protecting the confidential data stored in a database. Incorrect modifications of data, either intentional or unintentional, result in an incorrect database state. Incorrect modifications can be made intentionally by of attacker.

An attacker can be categorized into three classes:

- *Administrator*

An administrator is a person who has privileges to administer a computer system, but uses her administration privileges illegally according to organization's security policy to spy on DBMS behavior and to get valuable information.

- *Intruder*

An intruder is a person who is an unauthorized user means illegally accessing a computer system and tries to extract valuable information.

- *Insider*

An insider is a person who belongs to the group of trusted users and makes abuse of her privileges and tries to get information beyond his own access rights.

An attacker, after breaching through all levels of protection, he will try to do one of the two following attacks:

- *Passive Attack*

In passive attack, attacker only observes data present in the database. Passive attack can be done in following three ways:

  - *Static leakage*: In this type of attack, information about database plaintext values can be obtained by observing the snapshot of database at a particular time.
  - *Linkage leakage*: Here, information about plain text values can be obtained by linking the database values to position of those values in index.
  - *Dynamic leakage*: In this, changes performed in database over a period of time can be observed and analyzed and information about plain text values can be obtained.

- *Active Attacks*

  In active attack, actual database values are modified. These are more problematic than passive attacks because they can mislead a user. There are some ways of performing such kind of attack which are mentioned below:

  - *Splicing* – Here, a cipher text value is replaced by different cipher text value.
  - *Spoofing* – In this type of attack, cipher text value is replaced by a generated value
  - *Replay* – Replay is a kind of attack where cipher text value is replaced with old version previously updated or deleted.

Attacks on database can also be classified into direct and indirect attacks:

- *Direct attacks*

A direct attack means attacking the target directly. These are obvious attacks and are successful only if the database does not implement any protection mechanism. If this attack fails, the attacker moves to the next.

- *Indirect attacks*

Indirect attacks are the attacks that are not directly executed on the target but information from or about the target can be received through other intermediate objects. Combinations of queries are used some of them having the purpose to cheat the security mechanisms. These attacks are difficult to track.

II. SECURITY THREATS TO DATABASE

- *Privilege insecurity*

Required privileges are given to database users by database administrator which is used on daily basis like permission to create table, right to select rows from another user's table, right to database, permission to query a table etc.; but sometimes these authorities are misused by users intentionally or unintentionally**.** Having seen how privilege can be abused intentionally, let assume it with an example. A bank is providing a "granting loan "option to its manager and he takes a backup of sensitive data to work on from his home. This violates the security policies of the organization.

- *Platform vulnerabilities*

Vulnerabilities in operating systems and additional services installed on a database server may lead to unauthorized access, data corruption or service denial. This could be prevented by updating the operating system security.

- *Tampering of data*

In a distributed environment, it may be possible that an unauthorized third party can perform crime by tampering with data as it moves between sites. In data modification attack, an unauthorized third party changes parts of that data before retransmitting it.

- *Buffer Overflow*

When a program or process tries to store more data in a buffer then it was intended to hold, this situation is called buffer overflow. Since buffers contains only a finite amount of data according to its size, the extra data - which has to go somewhere - can overflow into adjacent locations, corrupting or false changes unintentionally on the valid data held in those locations.

- *Weak Audit Trails*

A database audit policy ensures automated, timely and proper recording of database transactions. It also helps in analysis of information held on servers for authentication, accounting and access of a user. Such a policy should be a part of the database security considerations since all the sensitive database transactions have an automated record and the absence of which is a serious risk to the organization's databases. There can be a serious organizational risk without good audit policy on database.

- *Weak Authentication*

Authentication is the basic necessity. To ensure security, the identity is authenticated and it keeps the sensitive data secure and from being modified by any ordinary user. With weak authentication models allow attackers to employ strategies such as social engineering and force to obtain database login credentials and assume the identity of legitimate database users.

III. DATABASE PROTECTION REQUIREMENTS

There are three elements that are considered as the most crucial components of security.

- *Confidentiality:*

Confidentiality can also be called privacy. Different privacy measures are applied on database to ensure confidentiality to save data from unauthorized people. Users are provided access to useful and confidential information; before granting any access to data system identify the user to confirm the identity of correct person. Only authenticated users can access or make request to data in database.

Sometimes safeguarding data confidentiality may involve special training for rookies on those documents. On that time many security risks can be there while training is given on those documents. Training can help familiarize authorized people with risk factors and how to guard against them. Training can include strong passwords and password-related best practices to guard data or information.

- *Integrity*

Integrity involves entry of valid data to obtain security of database. It also maintains consistency and accuracy of data; so that data can not changed by unauthorized people. It consists of the following aspects:

- *Integrity constraints*: These are applied to maintain the correctness and validity of the data in the database.
- *System and object privileges*: DBA grant privileges to the user who need to use the system and classify users and data in accordance with the policy of the firm. So that only authorized users can modify data.
- *Protection from viruses*: Database must be protected from different kinds of viruses by using protection measures like antivirus, firewalls etc.
- *User access controls*: It ensures that access to the network is controlled and safe during transmission across the network.

- *Availability*:

Availability refers data should always be made available for the authorized users by the secure system without any delay. Resources are managed by the users who are working on databases; so that data within database is available all the times to all the valid users. It has following aspects:

- *Easy to use*: Resources should be properly managed to make it available all the time to all the valid users so that it becomes easy to use.
- *Scalability*: System should not be degraded its performance with the increase number of users which require services from the system.
- *Flexibility*: Administrators must have all the mechanisms that are necessary to manage the information of the users and their access rights etc.

IV. VARIOUS MECHANISMS FOR DATABASE PROTECTION

- *Authorization*

Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use.
A person who owns the data is called authorizer in most cases DBA. In authorization user get authority or privilege of several access rights on database objects (e.g. Database tables, views, triggers etc). Several kind of authorization on part of database is given to user such as authority to manipulate data with various operations such as read, write, delete and update.

- *Views*

View is also called virtual table. View contains several fields from one or more real tables in database. It is a powerful and flexible security mechanism as it hides parts of databases from certain users. JOIN statements, WHERE condition and SQL function can also be added to view.
Syntax of creating view:
CREATE VIEW view_name AS
SELECT column_name(s)
FROM table_name
WHERE condition
Example of creating view:
CREATE VIEW emp_view as select emp_name, deptt_id from employee where emp_id = #123;
With above example authorized user can see this view by following command:
Select * from emp_view;

- *Access Control*

It plays a vital role in database protection. It is an aspect of database security which specifies that which part of data is accessed by whom. Different techniques like privileges, roles, and user accounts are available to control on data access.
There are two types of approaches which are used for database protection.

- Mandatory access control: In this approach data and users are classified into various security classes to enforce multilevel security.
- Discretionary access control: In this approach data files or fields in a specific modals that are accessed by users who are given some kinds of privileges.

- *Database Encryption*

Encryption is the technique of transforming information by means of a cipher so that it becomes unreadable to all other people except those who hold a key to the information or we can say that it is a technique in which sensitive data is first encoded and then transmitted. At destination or receiving end data is then decoded. Security is increased by this method. It becomes very difficult to extract information by unauthorized users. As time performance degrades in decoding of encrypted data it also has following features:

- It is a simple method of data protection from unauthorized access
- It is very difficult for an intruder to determine the encryption key.

- *Integrity constraints*

To prevent invalid entries in tables of database there are different integrity constraints. It returns error if anybody try to violate the rules with different DML statements like insert, delete, update and select. The different kind of integrity constraints are:

- NOT NULL integrity constraints
- Primary key integrity constraints
- Foreign key integrity constraints
- Unique key integrity constraints
- Check integrity constraint

- *Back-up*

An organization could face harmful results if the data stored in database crashed due to internal or external factors. So it becomes necessary to recover that useful data to protect from these kinds of disasters. So to reconstruct the lost data back up plans should be there. We can have checkpoints at multiple stages so as to save the contents of the database periodically.

- *Privileges*

Privileges are special or required authorities given to users by the system/database administrator. There are two types of privileges:

- *System privileges*: In this category each account hold particular object and perform particular action on that object in the database independently so it is also called account level privilege. Examples of system privileges are *create table, create session, create view, alter procedure* and *drop privilege* etc.
- *Object privileges*: This category is used to manipulate and access database objects by user. User can do manipulations on objects like view, procedure, sequence, functions etc. Different functions that can be applied on objects are *insert, update, delete etc*.

V. CONCLUSION

In this paper various issues of database security are discussed. Every organization needs to protect its sensitive data from unauthorized access. There are lots of threats that can harm data; to save data stored in database from harm or insecurity different techniques mentioned above in this paper which are recently used for database protection.

REFERENCES

[1] R. Agrawal, R. Srikant, and Y. Xu, "*Database Technologies for Electronic Commerce*," Proc. Very Large Databases Conf. (VLDB), 2002.

[2] R. Ahad, J. Davis, S. Gower, P. Lyngbaek, A. Marynowski, and E. Onuegbe, "*Supporting Access Control in an Object-Oriented Database Language*," Proc. Int'l Conf. Extending Database Technology (EDBT), 1992.

[3] M.M. Astrahan, *et. al.* "*System R: A Relational Approach to Database Management*," ACM Trans. Database Systems, vol. 1, no. 2, pp. 97-137, 1976.

[4] S. Singh, *Database systems: Concepts, Design and Applications*, New Delhi: Pearson Education India, 2009.

[5] S. Sumanthi, Fundamentals of relational database management systems Berlin: Springer, 2007.

[6] Jeffery D. Ullman, *Principals of Database System*, Galgotia Publications, 1996.

[7] Abraham Silberschatz et al, *Database System Concepts*, McGraw-Hill.

[8] C.J.Date, *An Introduction to Database Systems*, Addison-Wesley Publishing Company, Inc.

[9] DBMS-Data Backup. [Online] Available at: http://www.tutorialspoint.com/dbms/dbms_data_backup.htm

[10] Bright Hub, Types of Threats to Database Security. [Online] Available at:http://www.brighthub.com/smb-security/articles/61554.aspx

[11] A. Gupta, *et. al.* , *Fundamentals of DBMS*, Lakhnpal Publishers,2008.