UNIT ⇒ '5'

Database Security.

Abhay Kumar Mishra
Lecturer, Dept. of B.C.A.
Maharaja College, Ara (M.U.S.U.)

Database Integrity is the preservation of data correctly (data) & implies the process of keeping the database from an accidental dilution or alteration. (change data)

(The extent to which the data used for processing are reliable accurate, & free from error).

Integrity Rules & constraint.

- Relation database model specifies the following integrity constraint :-)

1) Entity Integrity constraint (field) :-)

Every Record must have value in primary key field.

Primary key value must be unique.

2) Referential Integrity :-)

i) It is concerned with the concept of foreign key field or constraints.

ii) References primary key field in another table.

iii) Specified when creating tables.

Abhay Kumar Mishra
Lecturer, Dept. of C.S.
Maharaja College

3) Domain Integrity Constraint :-

Domain Integrity Constraint specifies that the value of an attribute, say A, must be from the domain (A). A domain is a set of atomic values.

For the domain for the attribute Age as Emp. table will be the set of all possible positive numbers, between 60 & 65. The attribute can not hold a value other than those specified in the domain.

* Database Security :-

Database Security includes policies framed to protect data falling in the hands of unauthorized users.

Security also includes the technique used to ensure that data elements are not changed or deleted by viruses or by unauthorized person.

- In short data security addresses the following issues:-

a) Privacy of certain data elements.

b) Preserving policies of the organisation.

c) System related security level.

d) Maintaining Integrity of database.

* Authorization
* Identification (पहचान)
* Authentication. (प्रमाण)
* Encryption decryption
* Integrity rules & constraint.
* Auditing.

* Security Consideration in DBMS *

1) Authorization (a, c)

The restricting database access only to authorized users can be implemented by the access control mechanism.

Access control is made available by creating user's A/c & password.

The Data base Administrator (DBA) has the responsibility of granting access permissions & user A/c to various users of a database.

- DBA has the following responsibilities is)

1) Creating a new A/c & password for a user or a group of users (A/c creation).

2) Allowing a user A/c to have access to certain part of database (Privilege Granting).

3) Take away the privileges from a user A/c that we previously given to him. (Privilege Revocation).

4) Assigning user A/c to the appropriate security level (Security level assignment).

Application programs are also considered users by the DBMS & are required to supply user A/c & password.

2) Authentication (प्रमाण, सत्यापन) & Identification (निशान)

Identification & Authentication of a user can be done through any of the following ~~ones~~ ~~methods~~ methods :-)

a) What you know?

The simplest & the most common method is the usage of user's A/c no. & password for ~~an~~ authentication proces

The database system may also ask the user one or more questions.

Only an authenticated user will have an right answers to each questions.

b) What you have :--

For the identification each user is given a badge, card or key to be used for identification purpose.

A password or question-answer scheme as above can be used for authentication purpose.

c) What you are :-

With the help of his/her physical or physiological characteristics, such as thumb print.

Abhay Kumar Mishra
Lecturer, Dept. of
Maharaja College

- Special I/P or O/P can be to identify a user.

Database Audit :-

Database System keeps track of all the operations that a user performs during a log-in session.

When a user login, the DBMS records the user's A/c number & then associates it with the terminal for which the logged in.

All operations done from that terminal are attributes to that user A/c number till the user logs-off.

If any tampering (unauthorized) with database is suspected, a database audit is performed.

Database audit consists of reviewing the database accesses & operations done by a user A/c during a certain period of time. When an illegal or unauthorized operation is found, the DBA can determine the A/c no. which performed such an operation.

A database log that is used mainly for security purposes is called an Audit Trail.

* **Database Recovery** :- Database Recovery means that the entire data item in the database are restored to the most recent consistent state of the database as it was, just before the time of failure.

* **Recovery means** :- Restoration of database to the most recent correct state, if a failure occurs.

For this the system keeps record the changes by transaction in the database, in a log.

An ideal strategy for recovery is following:-

a) If there occures a wide damage to the database, due to disk crash or fire, the recovery method restores a past copy of the database from the archive storage. All the committed transactions in the log file are then re-done on this restored database.

b) If the database is not physically damaged, but has became erratic due to some logical error or system crash, the recovery method consist undo log.

Abhay Kumar Mishra
Lecturer, Dept. of B.C.A.
Maharaja College, Ara (V.K.S.U.)

the operations them at second the server. For such case, data in archives storage is not recorded, only the log file is required for doing.

Data Encryption & decryption :-

* The process of storing data is confidential data in a database in an encrypted (coded) form.

This encrypted data can not be read by anyone unless he knows how to decrypt it.

The process requires an encryption device to for converting the original message into a meaningless code.

* The process of converting meaningless code into the original message is called Decryption.

Decryption device for translating the code back into the original text.

* For the data process, this can accomplished by using specialized computer s/ws.

- A Good Encrypting algorithm has the following features:-

1) It should be very simple for authorized users to encrypt & decrypt data.

2) It is very difficult to keep the algo secret. Hence, the security of data should not depend on the secrecy of the algo, but on a parameter of the algorithms.

This parameter is known as key. The key should be knows only to authorized users.

3) The key used should be very difficult for an instructer to determine.

Identification & Authentication of a usr can be done through any of the following method.

a) What you know :-

The simplest & the most common method is the usage of usr A/c-no. & password for authentication purpose.

Ankur Kumar Mishra
Lecturer, Dept. of B.C.A.
Maharaja College, Ara (V.K.S.U.)

b) · What you have ?)

Each user is given a badge, card or key to be used for identification purpose.

c) What you are ?)

Special H/w or S/w can be used to as his/her physical or physiological characteristics such as thumb print.