

Data Security In Distributed Database & Semantic Integrity Control

RAMNA SATTAR



Data Security In Distributed Database

Data Security In Distributed Database:

Data security is an important function of a database system that protects data against unauthorized access. Data security includes two aspects: data protection and access control. Data protection is required to prevent unauthorized users from understanding the physical content of data. This function is typically provided by file systems in the context of centralized and distributed operating systems. Access control must guarantee that only authorized users perform operations they are allowed to perform on the database.

There are two main approaches to database access control

- 1. Discretionary access control**
- 2. Multilevel Access Control**



Data Security In Distributed Database

1. Discretionary access control :

Discretionary access control(or authorization control) defines access rights based on the users, the type of access (e.g., SELECT, UPDATE) and the objects to be accessed.

Three main actors are involved in discretionary access control control:

- subject (e.g., users, groups of users) who trigger the execution of application programs;
- operations, (Select , update, insert or delete)
- objects, on which the operations are performed (relations or attributes)



Data Security In Distributed Database

2. Multilevel Access Control:

Security levels arranged in Linear Order

- Top Secret [highest]
- Secret
- Confidential
- Unclassified [lowest]



Distributed Access Control

Distributed Access Control:

The additional problems of access control in a distributed environment stem from the fact that objects and subjects are distributed and that messages with sensitive data can be read by unauthorized users.

These problems are:

- remote user authentication,
- management of discretionary access rules
- handling of views and of user groups,
- enforcing multilevel access control



Distributed Access Control

Distributed Access Control:

Three solutions are possible for managing authentication:

- 1)** Authentication information is maintained at a central site for global users which can then be authenticated only once and then accessed from multiple sites.
- 2)** The information for authenticating users (user name and password) is replicated at all sites in the catalog. Local programs, initiated at a remote site, must also indicate the user name and password.
- 3)** All sites of the distributed DBMS identify and authenticate themselves similar to the way users do. Intersite communication is thus protected by the use of the site password. Once the initiating site has been authenticated, there is no need for authenticating their remote users.



Semantic Integrity Control

➤ Semantic Integrity Control

A database state is said to be consistent if the database satisfies a set of constraints, called semantic integrity constraints. Semantic integrity control ensures database consistency by rejecting update transactions that lead to inconsistent database states.

The integrity constraints are as follows –

- **Data type integrity constraint**
- **Entity integrity constraint**
- **Referential integrity constraint**

1. Data Type Integrity Constraint:

A data type constraint restricts the range of values and the type of operations that can be applied to the field with the specified data type.



Semantic Integrity Control

2. Entity Integrity Control:

Entity integrity control enforces the rules so that each tuple can be uniquely identified from other tuples. For this a primary key is defined. A primary key is a set of minimal fields that can uniquely identify a tuple. Entity integrity constraint states that no two tuples in a table can have identical values for primary keys and that no field which is a part of the primary key can have NULL value.

3. Referential Integrity Constraint:

Referential integrity constraint lays down the rules of foreign keys. A foreign key is a field in a data table that is the primary key of a related table. The referential integrity constraint lays down the rule that the value of the foreign key field should either be among the values of the primary key of the referenced table or be entirely NULL.



Centralized Semantic Integrity Control

Centralized Semantic Integrity Control

A semantic integrity manager has two main components: a language for expressing and manipulating integrity assertions, and an enforcement mechanism that performs.

Two basic methods permit the rejection of inconsistent update transactions.

- ❑ The first one is based on the **detection of inconsistencies**.
- ❑ The second method is based on the **prevention of inconsistencies**.



Distributed Semantic Integrity Control

Distributed Semantic Integrity Control

Definition of Distributed Integrity Constraints

- **Individual constraints:** single-relation single-variable constraints.
- **Set-oriented constraints:** include single-relation multivariable constraints such as functional dependency
- **Constraints involving aggregates:** require special processing because of the cost of evaluating the aggregates



THANK YOU

ANY QUERY???

