Distributed database security

Law, Security

Database management system usually runs at the top of operating system which provides security services to the database in the system. The following are some of the features need to be observed in operating system: memory and file protection, resource access control and user authentication. Memory protection will prevent memory of different program from interfering with the other and also limit accessibility of objects by employing memory segmentation technique.

The most important security requirements for database management system are; Multi-level Access control, confidentiality, reliability, recovery and integrity. Distributed database A distributed databases system comprises of the following, distributed database management system (DDBMS), a distributed database and network for system interconnection. A data which is distributed across multiple databases is what we term as a distributed database explained by Paul and Peter (2001). Functional requirement for Secure distributed database.

The following are the functional requirement need in distributed database they are; distributed query management, distributed transaction processing, distributed metadata management, security enforcing and integrity across multiple nodes. Distributed database system is built in a number of architecture, we have control which is centralized and data is distributed. Other architecture have data and control been distributed. The DDBMS manages distributed data. We have a Multi-database architecture in which each local database is managed by local DBMS with other DBMS connected to through a DDBMS.

DDBMS have a distributed query processor (DQP) this will deal with distributed queries, Distributed transaction manger (DTM) process distributed transaction, Distributed metadata manager (DTM) manages distributed metadata, and distributed integrity manager (DIM) enforces integrity constraint across the database and distributed security manager (DSM) which enforces security constraint across the databases discussed by Simon (2001). Authentication and Identification of user To identify the authentic user we apply access control rules.

The uses of SQL language which have the grant access to user and revoke access to user some data. It uses password approached to ascertain authenticity and identification of a user who is locking into the system Multilevel access control The multilevel security is requirement need on distributed databases, the approach is based on the distributed data and centralized control. Initially this approach was referring to partitioned approach where by a trusted front-end databases system is connected with non-trusted back-end database system.

Each and every trusted frond-end database system operates on single level and manages data on the same level. In this case unclassified DBMS will manage unclassified data and secret DBMSS manages secret data. The communication between backend database systems will be through front-end database which is a trusted database. A query by user will be sent to DBMS at user level or below user level. Request update will be send only to DBMS at user level. When user secret query is send to secret and unclassified RDBMS, when secret user's update request will be sent only to secret DBMS.

Distributed data and distributed control. The multilevel protect distributed database management system (MLS/DDBMS), In this approach users will be cleared at different security levels access while data in distributed database will be shared at different security levels without causing security concerns. Under this architecture the MLS/DDBMS have several nodes which are interconnected by multilevel secure network. In the case of homogenous environment all nodes are identically designed with each node with capability of handling multilevel data. Every node has a MLS/DBMS, which manages local multilevel database.

Also every node has distributed processing component known as secure distributed process (SDP) those information which are sensitive will be taken care by this modules. Modules of SDP are; secure Distributed query processor (SDQP), Secure Distributed Transaction manager (SDTM), secure distributed Metadata manager (SDMM), secure Distributed Security Manager (SDSM) and Security distributed integrity manager (SDIM), For the security measures for multilevel to be reinforced should be appropriate security policy based on the local DBMS, network and distributed processor discussed by Ray (2001).

Security policy The security policy stated by MLS/DBMS I a policy of mandatory access control (MAC) and discretional access control which control access to data depend on the sensitivity level of data and clearance level of the user. Discretionary security measures are rules which specify access of various data given to users or group of user. There is also policy of integrity, identification and authentication, auditing and accounting. To make the system robust the algorithm for query, update and transaction processing in the DDBMS should be extended to multilevel security.