Dec 21, 2022

Plagiarism Scan Report

0% Plagiarized

100% Unique

Characters:1645

Words:265

Sentences:16

Speak Time: 3 Min

Excluded URL | None

Content Checked for Plagiarism

Due to the fact that other computerized system elements, such as the operating system, are also impacted, the security issue with databases cannot be viewed as an isolated issue. As a result, DBMS can adapt to many of the security models used for trusted OS. The formal explanation of security policy is what security models are. These are also valuable and significant resources for calculating and evaluating security policy. This security enhancement model serves to preserve the security of the database system in its typical architecture. The existing approach has a multilayer design, meaning there are two distinct layers: the Agent module and the Security detect module. The Agent Model receives the query first, and the Security Detect Model receives the results of this filter. The proposed system only has one layer. The data is not transferred from one module to another. In the suggested paradigm, this transition time is reduced. Execution time is decreased without compromising the system's security against internal threats, maintaining system security as-is. There are several features that make the proposed model secure and efficient to use. No user is able to access the data without permission. No user is able to change the data without permission. There is no mechanism in place that allows one person who is permitted to receive information to give that information to another user who is not. A method cannot be activated by any user without permission. The operating environment and the people involved are just as important to the security of the database as the security model or DBMS product that is selected.

Sources