NAME: SHRAVANI SUBHASH PAWAR

ROLL NO: A041

CONTROL ID: 2020080174

CLASS: TYBSC IT

SUBJECT: SECURITY IN COMPUTING

TOPIC: DATABASE SECURITY

Efficient and Effective Security Model for Database Specially Designed to Avoid Internal Threats

SUMMARY:

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.

On Distributed Database Security Aspects

SUMMARY:

The term "distributed database" refers to a collection of databases kept on different machines but often presented as a single database to applications. A distributed database system stores the database across multiple machines. Authentication, identity, and enforcing adequate access rules are the three most crucial security concerns.

Some of the most important security requirements for database management systems are:Multi-Level Access Control, Confidentiality, Reliability, Integrity, Recovery.

Most distributed database tools, including data warehouses, data mining systems, collaborative computing systems, distributed object systems, and the web, have an impact on security. The two primary problems with data warehousing systems are making sure that security is maintained while creating a data warehouse from the backend database systems and applying the right access control procedures when obtaining the data from the warehouse.

Next, data mining creates significant security issues. Building a retrieval controller that can recognise the user's intentions and stop the retrieval problem in its tracks is one way to solve the retrieval problem.

The security of the web has also received a lot of attention lately. Making sure that the databases, operating systems, applications, web servers, clients, and network are not only safe but also securely linked is the major concern in this situation.

Database Security Issues in Rough Relational Databases

SUMMARY:

Security is becoming increasingly important in database applications, especially in light of the extensive issues connected with identity theft and fraud, website visit history trackers, privacy and data mining apps, and the profusion of SPAM.

Numerous researchers have investigated problems with rough database security. Much of the research for fuzzy set databases also applies to the rough relational database because it, like the fuzzy database, allows for tuples that are not in the first normal form. Because the crude relational database allows sets of values for attributes, inherent security results. The overlap of query results that permits inference is one area of database security. The data in a relation may be altered to produce explicit associations for protected values.

The intersection of tuples in a single relation in a rough relational database cannot result in a security breach. There cannot be two tuples with the same interpretation since redundant tuples are not permitted in a rough relation.

From theorem: The intersection of tuples in a single rough relation R cannot lead to a security violation. It is clear that security in the rough relational database corresponds to uncertainty.

Database Security Threats and Challenges

SUMMARY:

The entire control of information, including deciding who will receive the data and how it will be used, is known as information security. Its importance increases from keeping privacy to preserving sensitive data like client accounts in banks. Powers to access it, and employing a set of technologies to ensure that it is not infiltrated by any party. Physical security measures, firewall use, encryption, and data monitoring are among the protection techniques used to ensure information security. Threats to security might come from external, internal, or partner outlets.

There are three different degrees of abstraction available for the database. An internal dimension, a logical (or conceptual level), and an objective (or view level) level are typically included in a three-dimensional perspective. The safety of the server can be threatened by accessing or changing private data, etc. compromising the website's functionality or seriously undermining the client's and the sector's credibility. Each IT system needs to be categorized based on the most crucial data it has gathered, analyzed, or disseminated.

Physical security is the first step in database security. Other internal and external threats to databases exist, including SQL Injections, DB Vulnerabilities and Misconfigurations, Denial of Service Attack, Unmanaged Sensitive Data, Database Backups Exposure, Excessive Database Privileges, and Malware. To track and prevent security issues, people must work carefully to develop flaws and embrace emerging technology.

Learning Database Security with Hands-on Mobile Labs

SUMMARY:

As mobile computing becomes more prevalent, the security dangers to mobile applications are multiplying rapidly. The majority of harmful activities not only steal a user's transactions and communications or contact and location information, but also hack the organization's data by taking use of the private information.

SQL injection into the SQL database and any other data leakages caused by a lack of input validation and inadequate data leak security are potential threats to data confidentiality. Databases need to be protected from viruses and security flaws. To improve the security learning in the field, the chosen laboratories have been integrated into a variety of computer courses, including database, mobile software development, and mobile app & security.

This paper outlines a method for giving students hands-on, authentic mobile experience while they learn about database security. Many students show their innovation by coming up with clear insight and fresh approaches to safeguard mobile apps and gadgets. The open source Android Java and lab integrality's short learning curve also make it possible for teachers to embrace them quickly and sustainably, which increases their IAS capacity. Students are given step-by-step interactive hands-on practice within the lab activity itself, which engages and motivates them to construct mobile apps or security solutions on their own mobile devices and increases their positive feelings through experiences of mastery.