

Assignment 7 :

Part 1.

Securing an SQLite database is the most important part of safeguarding sensitive data from potential security breaches and unauthorized access. The following are different types of ways that you can make sure that you limit the amount of security risks that your database is exposed to.

To begin with, creating robust authentication measures is essential. This involves enforcing strong passwords or employing encrypted keys to control access to the database. By doing so, the system ensures that only authorized individuals or applications can gain entry, thereby fortifying the first line of defense against malicious intruders.

The least privilege principle is another fundamental practice. By granting users and applications only the minimum required access rights, the database's capabilities are restricted. A breach or compromised account can be minimized by this approach, reducing the attack surface and providing security that is more resilient.

Data encryption is a critical aspect of database security. In order to prevent unauthorized individuals from accessing sensitive information, transparent data encryption techniques are employed. In the event that the underlying storage medium is compromised, this additional layer of protection ensures that the data remains confidential.

Keeping the SQLite software up-to-date is equally important. Updates and patches provided by the developers strengthen the database's resilience against emerging threats by addressing newly discovered vulnerabilities.

Managing SQL injection risks requires proper input validation and data sanitization. A database that validates user inputs and sanitizes data enhances overall security by preventing malicious code injections.

Physical security must be noticed, and the database should be stored in a secure location. Additionally, adding firewalls to control access to the database server aids in blocking unauthorized external connections, minimizing exposure to potential threats.

In conclusion, sticking to a type of multi-faceted security system is your best chance of making sure that your data is not only safe but secure as well. Some different ways that you can implement to secure your data are as follows: data encryption, regular updates, input validation, and robust physical security measures will significantly enhance the security posture of an SQLite database. By conscientiously implementing these measures, organizations can protect their critical data assets and maintain their databases' confidentiality, integrity, and availability in a more formal and professional manner.