Database Security

Database Security means to keep sensitive information safe and prevent the loss of data. Security of data base is controlled by Database Administrator (DBA).

The following are the main control measures are used to provide security of data in databases:

1. Authentication

2. Access control

3. Inference control

4. Flow control

5. Database Security applying Statistical Method

6. Encryption

These are explained as following below.

1.Authentication :

Authentication is the process of confirmation that whether the user log in only according to the rights provided to him to perform the activities of data base. A particular user can login only up to his privilege but he can’t access the other sensitive data. The privilege of accessing sensitive data is restricted by using Authentication .

By using these authentication tools for biometrics such as retina and figure prints can prevent the data base from unauthorized/malicious users.

2.Access Control :

The security mechanism of DBMS must include some provisions for restricting access to the data base by unauthorized users. Access control is done by creating user accounts and to control login process by the DBMS. So, that database access of sensitive data is possible only to those people (database users) who are allowed to access such data and to restrict access to unauthorized persons.

The database system must also keep the track of all operations performed by certain user throughout the entire login time.

3.Inference Control :

This method is known as the countermeasures to statistical database security problem.It is used to prevent the user from completing any inference channel. This method protect the sensitive information from indirect disclosure.

Inferences are of two types, identity disclosure or attribute disclosure.

4.Flow Control :

This prevents information from flowing in a way that it reaches unauthorized users. Channels are the pathways for information to flow implicitly in ways that violate the privacy policy of a company are called covert channels.

5.Database Security applying Statistical Method :

Statistical database security focuses on the protection of confidential individual values stored in and used for statistical purposes and used to retrieve the summaries of values based on categories. They do not permit to retrieve the individual information.

This allows to access the database to get statistical information about the number of employees in the company but not to access the detailed confidential/personal information about specific individual employee.

6.Encryption :

This method is mainly used to protect sensitive data (such as credit card numbers, OTP numbers) and other sensitive numbers. The data is encoded using some encoding algorithms.

An unauthorized user who tries to access this encoded data will face difficulty in decoding it, but authorized users are given decoding keys to decode data.

Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious cyber threats and attacks.

Database security procedures are aimed at protecting not just the data inside the database, but the database management system and all the applications that access it from intrusion, misuse of data, and damage.

It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment.

Database security covers and enforces security on all aspects and components of databases. This includes:

I. Data stored in database.

II. Database server.

III. Database management system (DBMS).

IV. Other database workflow applications.

Database security is generally planned, implemented and maintained by a database administrator and or other information security professional.

Some of the ways database security is analyzed and implemented include:

I. Restricting unauthorized access and use by implementing strong and multifactor access and data management controls.

II. Load/stress testing and capacity testing of a database to ensure it does not crash in a distributed denial of service (DDoS) attack or user overload.

III. Physical security of the database server and backup equipment from theft and natural disasters. Regular data backups can be planned as part of a database security protocol, and multiple copies can be stored off-site to provide redundancy and emergency recovery.

IV. Reviewing the existing system for any known or unknown vulnerabilities and defining and implementing a road map/plan to mitigate them.

V. Data encryption can provide an additional layer of security to protect the integrity and confidentiality of data.

Enforcing adequate database security practices is vital for any organizations for a variety of reasons. These include:

I. Ensuring business continuity: Many enterprises cannot operate until the breach is resolved.

II. Minimizing financial damage: Once a breach occurs, an organization must sustain significant financial costs to communicate the breach to all its customers, manage the crisis, repair or update the affected systems and hardware, pay for investigative activities, etc.

III. Loss of intellectual property: If a database is accessed, there’s a chance that a company’s trade secrets, proprietary procedures, and other forms of intellectual property are stolen or exposed. In some instances, this means the complete loss of any competitive edge maintained by that organization.

IV. Brand reputation damage: Once a breach is notified to the customer base, partners and customers may lose faith in the organization’s ability to protect their data. The brand’s reputation will suffer, and many might decide not to buy that organization’s products or services anymore.

V. Penalties and fines: Organizations must be compliant with a large number of regulations, such as those in the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and more. If a data breach occurs because the organization failed to comply with these regulations, fines and penalties can be very severe, in some cases even exceeding several million dollars per violation.