<u>Data Integrity Its Types, Aspects and Threats to it</u>

PROTECT YOUR DIGITAL WAY TODAY AND TOMORROW

Table of Contents

Data and Data Integrity

+ Data

Data refer to facts/statistics that are collected for analysis. These are units of information. Data are used in the functioning of businesses, in scientific research and in every form of organizational activity.

+ Data Integrity

The process that ensures accuracy and consistency of data in its life cycle is termed as data integrity. Data integrity has to do with any type of data collection. Data integrity takes care of the accuracy, completeness and consistency of data. It also entails ensuring the safety of data.

To digress, websites also have data. The data of websites are stored on the servers of web hosting companies and are delivered from there over the Internet to make websites accessible. Web hosting can be of many types and the most popular web hosting services are usually referred to as the "Best Cloud Hosting", the "Best Linux Shared Web Hosting", the "Best Linux Dedicated Hosting" etc.

Types of Data Integrity

Data integrity encompasses various types. These are mentioned below.

+ **Physical integrity-** Physical integrity of data refers to protecting the thoroughness and accuracy of data during its storage and retrieval. Data's physical integrity is compromised when any untoward incident takes place, such as a natural disaster, hacking etc.

+ **Logical integrity-** Logical integrity ensures that data remains unaltered during its usage in various ways in a relational database. Data is protected by it from hackers and human errors. Logical integrity's way of protection differs from that of physical integrity. This type of data integrity can be of four types, which are entity integrity, domain integrity, referential integrity and user-defined integrity. Information on each of these will be provided in the next slide.

Types of Logical Integrity Explained

The four types of logical integrity are explained below.

+ **Entity integrity-** This type of logical integrity functions by creating primary keys/unique values for identifying data in order to ascertain that data doesn't get listed more than a single time. It also ensures that there isn't any field in a table that remains null.

+ **Domain integrity-** Domain integrity is a collection of processes for ensuring data's accuracy in a domain.

+ **Referential integrity-** Referential integrity includes a series of processes for ensuring uniform storage and usage of data. In it rules are embedded into the structure of a database with regard to the usage of foreign keys. This ensures that data-related changes, deletions or additions are appropriate.

+ **User-defined integrity-** This type of logical integrity includes the rules and constraints that are created by users for their requirements.

+

Threats to Data Integrity

The threats to data integrity can result from the following-

+ **Damage while in transit-** Data can get damaged during transfer over a network.

+ **Configuration issues-** Configuration issues in a system can damage data.

+ **Hardware failure-** Failure in hardware, such as a storage device can cause data damage.

+ **Human error-** Mistakes by humans can damage data.

+ **Intentional breach-** Data can be damaged deliberately by a person or through a software.

Aspects of Data Integrity

The time, date and identity of the one that recorded data should be present in it.

+ Data should be easy to read.

+ It should be easy to format data.

+ Data should be recorded in real time.

+ Data should be maintained in its original format.

+ Data should be maintained securely and be backed up.

+ Data should not contain any error.

+ Data should follow protocols.

Practices to Ensure Data Integrity

+ **Validating input-** Input should be checked when it is recorded. Digital input should be automated. Input validation can serve the purpose of blocking cyberattacks.

+ **Validating data-** The collected data is in raw form. Data validation ascertains the quality of data with regard to it being meaningful, correct and secure. Digital validations can be automated through the use of scripts for filtering and organizing data.

+ **Maintaining backups-** An efficient backup maintains a copy in a different location. Original raw data should be included in backups.

+ **Implementing access controls-** It should be ensured that access to data depends on business needs. Unauthorized access to data should be restricted. Limited access to data lowers the chances of data loss.

+ **Maintaining an audit trail-** An audit trail should be maintained which records data access and usage. An audit trail proves to be useful for identifying data loss' source.

Thanks!