



Database Security

Sensitive data, Inference, Multilevel Security

By

Prof. Muhammad Iqbal Bhat

Department of Higher Education

Government Degree College Beerwah

Prof. M. Iqbal Bhat (JKHED)

Topics



Sensitive data



Inference



Multilevel
Security

Prof. M. Lalal Bhat (JKHED)

Sensitive Data:

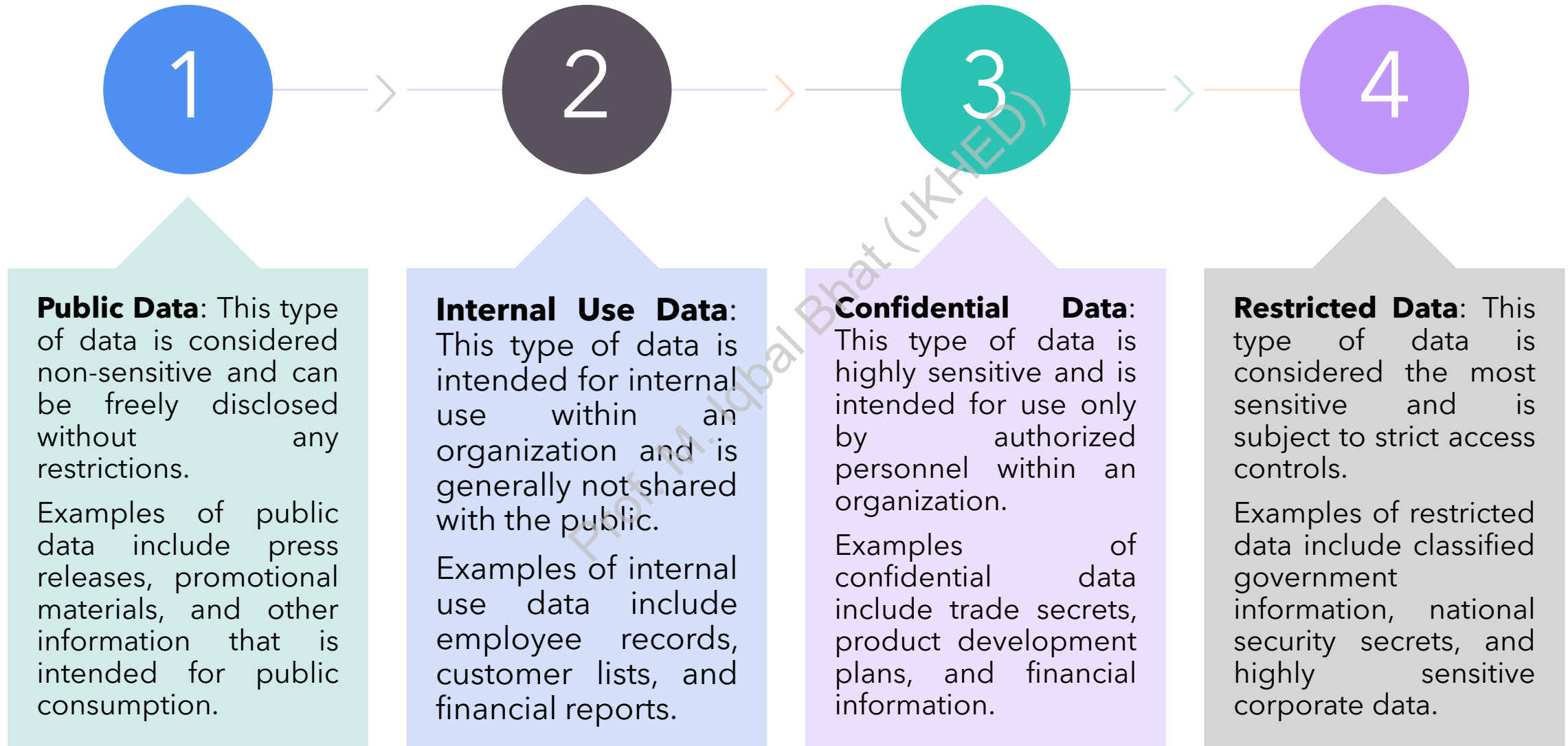


Sensitive data is any type of information that, if disclosed, could cause harm to an individual, organization, or society as a whole. This includes data that is confidential, personal, or proprietary in nature.



Examples of sensitive data include financial records, such as credit card numbers, bank account information, or tax identification numbers; health records, such as medical history or diagnoses; intellectual property, such as trade secrets, patents, or copyrights; and personal identifiers, such as social security numbers or driver's license numbers.

Types of Data based on Sensitivity:



Protection of Sensitive Data:

Protecting sensitive data is a critical aspect of database security. Sensitive data should be encrypted when stored and transmitted, and access to it should be restricted to authorized users only. Access controls should be implemented to ensure that users only have access to the data they need to perform their job functions.

In addition to technical controls, organizations should have policies and procedures in place to govern the handling of sensitive data. This includes training employees on security best practices, performing regular risk assessments and audits, and having incident response plans in place to address security breaches or incidents involving sensitive data.

Prof. M. Iqbal Bhat (JKHED)

Inference:



Inference is a method of deducing sensitive information from non-sensitive data through a series of logical or statistical analyses.



Inference attacks can be carried out by an attacker who has access to a database that contains both sensitive and non-sensitive data. By analyzing patterns in the non-sensitive data, an attacker can make inferences about the sensitive data.

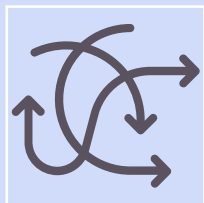


For example, if a database contains medical records that include a patient's age, gender, and zip code, an attacker could use statistical analysis to deduce information about the patient's medical condition or treatment history.

Inference:



Inference attacks can also be carried out through a combination of data from multiple sources. By correlating data from different sources, an attacker can make inferences about sensitive data that may not be present in any single source.



Inference attacks can be difficult to detect because they do not involve direct access to sensitive data. Instead, they rely on patterns and correlations in non-sensitive data to deduce sensitive information.

Measures to prevent inference attacks


Data Masking and Perturbation: Organizations can use data masking and perturbation techniques to add noise or randomization to non-sensitive data to make it more difficult for attackers to deduce sensitive information. For example, a medical database might use a technique called k-anonymization to group patients with similar demographic data and medical conditions, making it more difficult for an attacker to identify an individual patient's medical history.

Data Partitioning and Separation: Organizations can partition data into smaller subsets and separate sensitive data from non-sensitive data to limit the amount of information available in any single source. This can reduce the likelihood of an attacker being able to make inferences by correlating data from multiple sources.

Access Controls and Auditing: Access controls can be used to restrict access to sensitive data and limit the ability of attackers to make inferences from non-sensitive data. Auditing can be used to monitor access to sensitive data and detect any unauthorized attempts to access or manipulate the data.

Measures to prevent inference attacks

Regular Security Reviews: Regular security reviews can help organizations identify potential vulnerabilities and gaps in their security controls and procedures. This can help prevent inference attacks by ensuring that security measures are up-to-date and effective.



Education and Training: Employees and users should be educated and trained on security best practices and the risks associated with inference attacks. This can help prevent unintentional disclosures of sensitive data and improve overall security awareness within the organization.

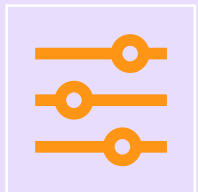
Multilevel Security:



Multilevel security (MLS) is a security model that allows for the simultaneous access of information with different levels of sensitivity, while enforcing strict access controls to ensure that each user can only access information at their level of clearance.



MLS is commonly used in government and military settings, where different levels of security clearance are required to access classified information.

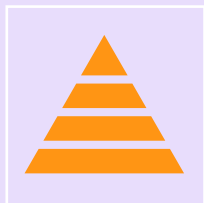


MLS works by assigning security levels to data and users based on their level of clearance. Each security level is defined by a set of security controls and policies that restrict access to the data based on the user's clearance level.

Multilevel Security:



For example, a government database might contain classified information at different levels of sensitivity, such as top secret, secret, and confidential.



Users with top secret clearance would be able to access all levels of classified information, while users with secret clearance would only be able to access secret and confidential information.

Implementation of MLS

MLS can be implemented through a variety of technical controls, such as mandatory access controls (MAC) or discretionary access controls (DAC). In MAC, access controls are enforced by the operating system or database, while in DAC, access controls are left to the discretion of the user or administrator.

MLS can be challenging to implement and maintain, as it requires strict security policies and procedures, as well as specialized training for users and administrators. Additionally, MLS can have a significant impact on performance and usability, as users may be required to undergo multiple authentication and authorization processes to access information at different levels of clearance.

However, MLS can provide a high level of security and control over sensitive information, making it an important tool for organizations that deal with classified or sensitive data.

attacks based on sensitive data, inference, and multilevel security

Attack Type	Example Attack	Date	Attack Description
Sensitive Data	Marriott International data breach	2018	A cyber attack resulted in the exposure of sensitive information, including passport numbers and payment card information, for over 500 million customers.
	Equifax data breach	2017	A cyber attack resulted in the exposure of sensitive information, including Social Security numbers and birth dates, for over 140 million people.
Inference	Harvard University data breach	2021	A hacker accessed sensitive research data, including confidential information about COVID-19 research, from Harvard University's research computing environment.
	Uber data breach	2016	A cyber attack resulted in the exposure of sensitive information, including names, email addresses, and phone numbers, for over 57 million users.
Multilevel Security	SolarWinds supply chain attack	2020	A hacker inserted malicious code into software updates for SolarWinds' Orion platform, allowing them to access sensitive information from multiple organizations, including government agencies and tech companies.
	Office of Personnel Management data breach	2015	A cyber attack resulted in the exposure of sensitive information, including Social Security numbers and background investigation records, for over 20 million government employees and contractors.



Prof. M. Iqbal Bhat (JKHED)

Questions?

