# ABSTRACT:

Organizations become more vulnerable to security breaches as they rely more on, potentially distributed, information systems for day-to-day operations, even as they gain productivity and efficiency benefits. Though there are currently a number of techniques available to protect data during transmission between sites for enforcing access control policies based on data contents, subject qualifications and characteristics, and other relevant contextual information, such as time which is a truly comprehensive approach to data protection must also include mechanisms. It is now widely accepted that the semantics of data must be considered when developing effective access control policies. Techniques for data integrity and availability that are specifically tailored to database systems must also be implemented. In this regard, the database security community has developed a variety of techniques and approaches over the years to ensure data confidentiality, integrity, and availability. Nonetheless, despite such advancements, the database security field faces a number of new challenges. Factors such as the growth of security concerns, data "disintermediation," new computing paradigms and applications such as grid-based computing and on-demand business have generated new security needs as well as new settings in which to apply and perhaps expand present techniques. In this paper, we will first cover the most significant ideas underpinning database security, followed by a description of the most often utilized approaches. We focus on access control systems, which have received a lot of attention in the literature, and identify key access control models, such as discretionary and mandatory access control models, as well as the role-based access control (RBAC) model. We next go through current database security issues and some tentative ways to tackle some of these challenges.

# INTRODUCTION:

As organizations increasingly rely on database systems as the primary data management technology for day-to-day operations and decision making, the security of the data managed by these systems becomes increasingly important. The recent rapid proliferation of Web-based applications and information systems has increased the risk exposure of databases, making data protection more important than ever. It is also critical to recognize that data must be protected not only from outside threats, but also from insider threats. As a result, a comprehensive data security solution must meet the three criteria listed below: 1) secrecy or confidentiality refers to the protection of data against unauthorized disclosure; 2) integrity refers to the prevention of unauthorized and improper data modification; and 3) availability refers to the prevention and recovery from hardware and software errors, as well as malicious data access denials, which render the database system unavailable. These three requirements can be found in almost every application environment. Privacy can be implemented using information confidentiality techniques; however, ensuring privacy necessitates the use of additional techniques, such as mechanisms for obtaining and recording user consent. Furthermore, confidentiality can be achieved by preventing access to data, whereas privacy is required even after the data has been disclosed. A database management system's various components ensure data security (DBMS). An access control mechanism, in particular, ensures data confidentiality. When a subject attempts to access a data object, the access control mechanism compares the user's rights to a set of authorizations, which is typically specified by a security administrator. The authorizations are stated in accordance with the organization's access control policies. The use of encryption techniques, which are applied to data when it is stored on secondary storage or transmitted over a network, improves data confidentiality even further. The access control mechanism and semantic

integrity constraints work together to ensure data integrity. When a subject attempts to modify some data, the access control mechanism ensures that the user has the right to do so, and the semantic integrity subsystem ensures that the updated data are semantically correct. Data availability, particularly for data available on the Web, can be enhanced further by employing techniques that protect against denial-of-service (DoS) attacks, such as those based on machine learning techniques.

## DB Security Concepts:

Authentication:

Authentication is the process or act of validating that a user is 1)attempting to log in to a database,

2)authorized to log in to a database. Example:

1. A cell phone provides authentication by requesting a PIN.
2. A computer verifies a username by prompting the user for the appropriate password. Authorization:

Authorization is a process of defining which users are allowed to access to the database, what privileges (access to which views, tables, attributes, how long...) of use in the database.

Examples:

The students are not allowed to modify their Academic Records in the University webpage. The students are allowed to view their Academic Records in the University webpage.

Data Confidentiality (Secrecy) : Data is not made available or disclosed to unauthorized individuals.

Example: DB stores Payroll Information - Not release/modify the individual salaries to/by unauthorized users.

Data Integrity:

Only defined and approved changes are made to data.

Example: A website of an airline Company - customer's reservations are not modified arbitrarily. Data Availability:

Data is available when needing to access. Prevention and recovery from making data be unavailable (Example: DDoS attacks)

Example: A website of an airline Company - The information on flight and reservations are always available.

## Introducing DB Security Approaches:

1)Authentication mechanism 2)Cryptographic techniques

1. Designed Features to detect, prevent, or recover from a security attacks
2. Recovery Subsystem & Concurrence Control
3. Access Control
4. Privacy-Preserving Techniques for Database 7)Privacy-Preserving Data mining

8)Privacy-Preserving Information Retrieval

Access Control:

A procedure for granting users access and particular rights to systems, resources, or information. All direct system accesses are subject to the rules established by security policies.

Use of Access Control:

Whenever a user tries to access a data object, Access Control checks the rights of the user against the set of authorization which states whether the subject can perform a particular action on the data object - Access Control ensures Data Confidentiality.

Whenever a user tries to modify some data, Access Control verifies the user has the right to modify the data - Access Control assures Data Integrity.

Whenever a subject tries to access a data object, Access Control checks the rights of the user against the set of authorization which states whether the subject can perform a particular action on the data object - Access Control ensures the Data Confidentiality.

Whenever a subject tries to modify some data, Access Control verifies the user has the right to modify the data - Access Control assures Data Integrity.

There are two Access Control Models:

1. Discretionary Access Control (DAC) 2)Mandatory Access Control (MAC) DAC:

A method of restricting object access depending on the identity of the persons and/or groups to which they belong. The term "DAC" refers to a sort of access control.

There are two tiers for granting access to the database system;

1. The account/system level: The administrator / DBA specifies the particular privileges that each account holds independently of the objects in the database system.

Examples: CREATE SCHEMA, CREATE TABLE, CREATE VIEW, ALTER, DROP, MODIFY, SELECT

1. The object level / relation (or table) level: The administrator can control the privilege to access each individual object in the database system (Data objects: Relation or View)

Examples: INSERT, UPDATE, DELETE, REFERENCE

Role Based Access Control (RBAC):

Constrained RBAC:

1. Add a requirement for enforcing separation of duty (SOD) SSD - Static SOD (based on user-role assignment)

Impose restriction on role intersections: 2 roles can not have common users.

1. Dynamic SOD - DSD (based on role activation) Limit the activation of roles during runtime.

RBAC in a commercial database management system: INFORMIX Online Dynamic Server Version 7.2

1. Sybase Adaptive Server 11.5.
2. Oracle Enterprise Server Version

Mandatory Access Control (MAC):

1. According to multilayer security (MLS):

Unclassified > Top Secret > Secret > Confidential

1. Subject has a security clearance of a given level.
2. Object has a security classification of a given level.
3. Two required properties for confidentiality: (Bell LaPadula) No read up (simple security property);

Class(S) >= Class (0)

No write down (star property); Class(S) <= Class(0)

Pros:

1. Ensure a high degree of protection, and prevent any illegal flow of information.
2. Suitable for military and high security types of applications. Cons:
   1. Require strict classification of subjects and objects 2)Applicable to few environments.

Privacy-Preserving Data Techniques: 1)Importance of data representation.

* 1. Increasing the number of data sets including Individual Data.
  2. Data availability causes serious threats for the privacy of Individuals and Organizations.
  3. Modifying the released data by removing items related to Individuals(data anonymity). Problems: The remaining data can be linked with other infos, so people can recover the privacy data.

Solutions: Generalizations Techniques (Relations to Fuzzy Concepts) Privacy-Preserving Data in Data Mining Context:

1. Causes: Data mining techniques may recover the removed information.
2. All approaches are based on modifying or perturbing data. 3)Developments are based on Commutative Encrypted Techniques. Hippocratic Databases:
   1. Incorporating privacy protection in relational database systems.
   2. Privacy policies stored in privacy-policy tables.
   3. Privacy authorization stored in privacy authorization tables.
   4. Privacy authorization defines authorized users.

## Database Security Challenges:

Data quality & Completeness:

Data quality: a perception or an assessment of data's fitness to serve its purpose in a given context.

Data Completeness: Data is not modified compared with the original. Techniques and organizational solutions:

1. Quality stamps.
2. Providing more effective integrity verification.
3. Tools for assessment of data quality. 4)Application-level recovery.

Intellectual Property Rights: (IPR)

1. Who create data.
2. Can be illegal to use this data. Techniques:
   1. Watermarking techniques for relational data are used to detect IPR violations. Database Survivability:
      1. Confinement: Actions to eliminate the attacker's access.
      2. Damage assessment: Determine the problem including failed function and corrupted data. 3)Reconfiguration: Run in safe-mode while recovery.
3. Repair:Recover data, reinstall failed system.
4. Fault treatment: Identify the weakness and prevent the recurrence of the faults.

Access control and privacy for mobile users:

1. Mobile is a popular and larger variety of devices available. 2)Computing power and sensor in the environment.
2. User with continuous online activities.
3. Personal information and become impotant key.
4. Need efficient storage, potable access rights. Techniques for mobile users:
   1. Access control mechanisms + standar for id management.
   2. Trust negotiation.
   3. Processing techniques for continuous queries.

# CONCLUSION:

Data security, particularly data protection from unauthorized access, is an important goal of any data management system. In this paper, we summarized research findings and practical developments, as well as discussed open research questions. Other relevant topics in the field of database security include inference control and statistical database security. Though these topics were researched several years ago, they remain relevant today, particularly in the context of privacy-preserving techniques. Other pertinent issues not addressed here include security for GIS data, which is becoming increasingly important for homeland security, information-grid architectures, and sensor data, as well as privacy and security for Web services and the semantic Web. All of these applications have interesting and novel security requirements that have largely gone unexplored.

# REFERENCES:

E. Bertino, S. Jajodia, and P. Samarati, “Database Security: Research and Practice,” Information Systems, vol. 20, no. 7, pp. 537-556, 1995.

E.B. Fernandez, R.C. Summers, and T. Lang, “Definition and Evaluation of Access Rules in Data Management Systems,” Proc. Very Large Databases Conf., 1975.

E.B. Fernandez, R.C. Summers, and C. Wood, Database Security and Integrity. Addison-Wesley, Feb. 1981.

E. Ferrari and B.M. Thuraisingham, “Security and Privacy for Web Databases and Services,” Advances in Database Technology—EDBT 2004, Proc. Ninth Int’l Conf. Extending Database Technology, Mar. 2004.

B. Thuraisingham, Database and Applications Security: Integrating Databases and Applications Security. CRC Press, Dec. 2004.

Database security-concepts, approaches, and challenges(2005)