ST. CLOUD STATE
UNIVERSITY™

Course Number: IA643

Professor: Dr. Jim Chen

# Security and Privacy Compliance: Challenges and Approaches

By

1.Makta Warsame (Student ID:13220223)

2.Gopi Thungam (Student ID:16178415)

3.Faozia Soukeina Traore (Student ID:13438556)

# ABSTRACT:

As organizations increasingly rely on distributed information systems to power their day-to-day operations, they gain efficiency but also become more vulnerable to security breaches. While distributed systems provide benefits, the data is more exposed when transmitted between different sites on a network. Currently there are several techniques used to safeguard data in transit, such as enforcing access controls based on attributes like data content, user qualifications, and contextual factors like time. However, a truly comprehensive approach to protection must also consider the semantic meaning and purpose of data, not just surface-level attributes. Database security researchers have long worked to develop database-specific solutions that ensure confidentiality, integrity, and availability of stored information. Over the years, they have introduced varied technical approaches and models to maintain these core aspects of security. Nevertheless, the field continues to face new challenges due to changing computing landscapes. Factors driving new risks include growing security concerns as attacks increase, data being used in more distributed and decentralized ways ("data disintermediation"), emerging technologies like grid computing, and business needs for flexible digital systems. These shifts necessitate not only applying existing techniques in new contexts, but potentially expanding technical strategies. Therefore, database security fundamentals and prevailing solutions need reexamination.

This paper aims to lay out foundational database security concepts and then analyze predominant access control approaches. A key focus will be models like discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). Finally, current database security issues introduced by technology and market trends will be surveyed. The paper also hopes to propose initial means of addressing some challenges, as safeguarding data in dynamic information systems remains critically important.In summary, the text outlines how database security research needs must evolve alongside computing transformations, analyzing traditional methods while scouting future innovation to maintain protection amid change. Let me know if any part warrants additional context or clarification.

# INTRODUCTION:

With the increasing reliance of organizations on database systems for day-to-day operations and decision making, the security of the managed data becomes a paramount concern. The proliferation of web-based applications and information systems has significantly heightened the risk exposure of databases, making data protection more critical than ever. It is essential to recognize that data must be safeguarded not only from external threats but also from insider threats. A comprehensive data security solution must address three fundamental criteria: confidentiality, integrity, and availability. Confidentiality ensures protection against unauthorized disclosure, integrity prevents unauthorized and improper data modification, and availability ensures the prevention and recovery from hardware and software errors and malicious denials of data access that render the database system unavailable. These requirements are crucial in almost every application environment. Privacy, although achievable through information confidentiality techniques, also necessitates additional measures such as obtaining and recording user consent. Moreover, privacy needs to be ensured even after data disclosure, unlike confidentiality, which focuses on preventing access to data. The components of a database management system (DBMS) collectively contribute to data security. Specifically, an access control mechanism plays a vital role in ensuring data confidentiality. When a subject attempts to access a data object, the access control mechanism verifies the user's rights against a set of authorizations specified by a security administrator, aligning with the organization's access control policies. Encryption techniques can further enhance data confidentiality by securing data stored on secondary storage or transmitted over a network. The access control mechanism and semantic integrity constraints work in tandem to ensure data integrity. When a subject seeks to modify data, the access control mechanism validates the user's authority to do so, while the semantic integrity subsystem ensures the correctness of the updated data from a semantic perspective. In the context of data availability, especially for web-accessible data, additional techniques can be employed to mitigate denial-of-service (DoS) attacks, such as those leveraging machine learning. To sum up, the present study centers on the methods and obstacles associated with privacy compliance and database

security. The importance of availability, secrecy, and integrity in data security is emphasized, along with the function of encryption methods, access control systems, and limitations on semantic integrity. It also discusses the significance of tackling new risks like DoS assaults and recognizes the necessity of privacy safeguards. This study seeks to offer important insights on guaranteeing security and privacy compliance in database systems by examining these factors.

## DB Security Concepts:

1. Authentication:

Authentication is a crucial security process used to verify a user's identity before granting access to sensitive information, like a database. This process ensures that the person seeking access is genuinely who they claim to be.

Example 1: When a user tries to access their mobile phone, the device may ask for a Personal Identification Number (PIN). This PIN is a simple form of authentication that confirms the user's identity.

Example 2: In the case of computer systems, authentication often involves verifying a username and password. When a user enters their username, the system prompts a password. This password must match the one associated with the username in the system's records to grant access.

2. Authorization:

Authorization, distinct from authentication, is the process of determining the level of access or permissions a verified user should have in a database or system. It involves defining what resources a user can access and what actions they can perform.

Example 1: In a university setting, students may have the authorization to view their academic records on the university's website, but they are not permitted to alter these records. This restriction ensures that the integrity of academic data is maintained.

Example 2: In a corporate environment, employees in different roles may have varying levels of authorization. For instance, while all employees can view certain common documents, only department heads may have the authorization to edit or approve them.

3. Data Confidentiality (Secrecy):

Data confidentiality refers to the protection of data from unauthorized access and disclosure. It ensures that sensitive information is only accessible to those who are permitted to see it.

Example: In the context of a company's payroll information, confidentiality is paramount. The

database storing payroll details must be designed to prevent unauthorized users from viewing or modifying individual salary information. This protection is critical for maintaining employee privacy and trust.

4. Data Integrity:

Data Integrity is about ensuring the accuracy, consistency, and reliability of data throughout its lifecycle. It means that data is kept intact, unaltered, and consistent from the point of its creation to the point of its delivery.

Example: Consider an airline's website, where customer reservations are stored. Data integrity in this scenario means that these reservations are not changed in an unauthorized or random manner. Only authorized personnel can make changes, and these changes are tracked and validated to ensure they are correct and intentional.

5. Data Availability:

Data Availability refers to ensuring that data is accessible when needed, regardless of any disruptions or challenges. It involves implementing systems and strategies to prevent and recover from circumstances that might render data inaccessible.

Example: On the website of an airline company, the flight information and reservation details must be always readily accessible to customers. This includes ensuring that the website is resistant to attacks like Distributed Denial of Service (DDoS) attacks, which can overwhelm and shut down servers, making data unavailable. Adequate measures such as robust server infrastructure, backup systems, and effective security protocols are essential to maintain continuous data availability.

## Introducing DB Security Approaches:

1)Authentication mechanism

2)Cryptographic techniques

3)Designed Features to detect, prevent, or recover from a security attack

4)Recovery Subsystem & Concurrence Control

5)Access Control

6)Privacy-Preserving Techniques for Database

7)Privacy-Preserving Data mining

8)Privacy-Preserving Information Retrieval

Access Control:

Access Control is a critical security measure in database management systems, designed to manage and restrict user access to system resources and information. It functions by adhering to security policies that dictate the rules for system access.

Functionality of Access Control in Database Security:

Protecting Data Confidentiality: It achieves this by evaluating a user's access rights whenever they attempt to view or interact with a data object. This evaluation, based on predefined authorization rules, is critical in preventing unauthorized access, thereby maintaining the confidentiality of the data.

Safeguarding Data Integrity: Similarly, Access Control is instrumental in preserving the integrity of data. It does so by scrutinizing whether users have the necessary permissions to alter data. This step is vital in preventing unauthorized data modifications, which could otherwise compromise data

accuracy and reliability.

There are two Access Control Models:

1)Discretionary Access Control (DAC)

2)Mandatory Access Control (MAC)

Discretionary Access Control (DAC):

DAC is a flexible access control method where access to database objects is based on the identity of users or the groups they belong to. The term "DAC" is indicative of a type of access control where the discretion for access lies with the owner of the resource or those designated by the owner. It operates on two primary levels:

System-Wide Access Management (Account/System Level):

At the broader account or system level, the DBA is responsible for defining user privileges across the database. These privileges encompass a range of actions from creating database structures like schemas and tables to modifying and selecting data, thereby dictating what each user can do within the entire database system.

Specific Data Object Access (Object Level/Relation Level):

On a more granular level, DAC allows administrators to control access to each individual data object, such as a specific table or view. This level deals with permissions related to data manipulation—such as inserting new records, updating existing ones, deleting records, or making references to data within these objects.

Role-Based Access Control (RBAC):

RBAC is a widely used access control mechanism in database systems. It assigns permissions based on roles rather than directly to individual users. Users are then assigned to these roles, simplifying permission management, and improving security.

Constrained RBAC:

Constrained RBAC enhances standard RBAC by incorporating rules that enforce separation of duties

(SOD), a critical aspect of internal controls to prevent fraud and errors:

Static Separation of Duty (SSD):

SSD is based on user-role assignments and imposes restrictions on role intersections. It ensures that two conflicting roles cannot be assigned to the same user. For example, the same user should not be allowed to have both the roles of 'Accountant' and 'Auditor' to prevent a conflict of interest.

Dynamic Separation of Duty (DSD):

DSD focuses on the activation of roles during runtime. It limits the simultaneous activation of certain roles to prevent misuse of privileges. For instance, a user may have multiple roles but can only activate a specific role under certain conditions or in specific contexts.

RBAC in Commercial Database Management Systems:

RBAC is implemented in various commercial database systems, providing robust access control options:

INFORMIX Online Dynamic Server Version 7.2:

This system utilizes RBAC to manage user access and privileges efficiently.

1.Sybase Adaptive Server 11.5:

Sybase Adaptive Server also integrates RBAC, allowing for role-based permission management.

2.Oracle Enterprise Server Version:

Oracle's Enterprise Server employs RBAC, facilitating secure and efficient user role management.

Mandatory Access Control (MAC):

MAC is a stringent access control model used primarily in high-security environments. It's based on multilevel security (MLS) and involves assigning security classifications to both users (subjects) and data (objects).

Multilayer Security (MLS):

MLS in MAC categorizes data and clearance levels in a hierarchy, such as Unclassified, Confidential, Secret, and Top Secret. This hierarchy ensures that sensitive information is accessible

only to those with appropriate security clearance.

Security Clearance for Subjects:

Every user or subject in a MAC environment is assigned a security clearance level. This clearance determines the highest level of information that the subject can access.

Security Classification for Objects:

Similarly, data or objects are assigned a security classification. This classification defines the sensitivity level of the information and who can access it.

Confidentiality Properties (Bell-LaPadula Model):

MAC adheres to the Bell-LaPadula model, which includes two critical properties for maintaining confidentiality:

No Read Up (Simple Security Property): A subject with a certain security clearance cannot read data classified at a higher level. For example, someone with 'Secret' clearance cannot access 'Top Secret' information.

No Write Down (Star Property): A subject cannot write information to a lower classification level. This prevents sensitive information from being inadvertently downgraded.

Pros and Cons of MAC:

Pros:

High Degree of Protection: MAC offers robust security, effectively preventing unauthorized access and information leaks.

Ideal for High-Security Environments: It is particularly suitable for military or other environments where information security is critical.

Cons:

Strict Classification Requirements: MAC requires rigorous classification of all subjects and objects, which can be complex and resource intensive.

Limited Applicability: Due to its strict nature, MAC is suitable for a limited range of environments, primarily where security is of the utmost importance.

Privacy-Preserving Data Techniques:

Importance of Data Representation:

The way data is represented and stored can significantly impact privacy. Effective data representation should balance the utility of data with the need to protect individual privacy.

Challenges with Increasing Individual Data in Datasets:

The growing volume of datasets containing individual data increases the risk of privacy breaches. As more personal data is collected and stored, safeguarding this information becomes increasingly critical.

Threats Posed by Data Availability:

While data availability is essential for analysis and decision-making, it also poses significant privacy risks. The widespread availability of data can lead to unauthorized access and misuse of personal information.

Data Anonymization Techniques:

Modifying released data to remove or obscure personal identifiers (data anonymization) is a common approach to protect privacy. However, challenges arise when anonymized data can be linked with other information to re-identify individuals.

Problems and Solutions in Privacy-Preserving Data Techniques:

Problems:

Even after anonymization, the remaining data may be linked with other sources, potentially compromising privacy.

Solutions:

Generalization techniques and the application of fuzzy concepts are used to further obscure data, reducing the risk of re-identification.

Privacy-Preserving Data in Data Mining:

Data mining often involves analyzing large datasets, which can lead to the recovery of removed or

anonymized information. To address this, methods such as modifying or perturbing data and using commutative encrypted techniques are employed.

Hippocratic Databases:

These databases integrate privacy protection into their core design:

Privacy policies are stored in dedicated privacy-policy tables.

Privacy authorizations, which define who is authorized to access specific data, are stored in privacy authorization tables.

This approach ensures that data access and usage align with established privacy policies and user consents.

## Database Security Challenges:

Data Quality & Completeness:

Data Quality: Refers to the suitability of data for its intended purpose in a specific context. High data quality is crucial for reliable decision-making and analytics.

Data Completeness:

1. Ensures that data remains unmodified and intact from its original state.

2.Techniques and Organizational Solutions:

3.Implementing quality stamps to certify the reliability of data.

4.Developing more effective methods for integrity verification.

5.Utilizing tools for the regular assessment of data quality.

6.Applying application-level recovery processes to maintain data integrity.

Intellectual Property Rights (IPR):

IPR concerns in databases revolve around who creates data and the legality of its usage.

Techniques:

Employing watermarking techniques for relational data to detect IPR violations and protect the rights of data creators.

Database Survivability:

Confinement: Taking actions to restrict an attacker's access following a security breach.

Damage Assessment:

Evaluating the extent of the damage, including failed functions and corrupted data.

Reconfiguration: Operating in a safe mode while recovery processes are underway.

Repair: Restoring data and reinstalling systems that have failed.

Fault Treatment: Identifying weaknesses and implementing measures to prevent similar issues in the future.

Access Control and Privacy for Mobile Users:

1.The ubiquity of mobile devices and their diverse capabilities pose unique challenges in terms of computing power, sensor integration, and continuous online activities.

2.Protecting personal information stored and accessed on these devices is critical.

Techniques for Mobile Users:

1.Implementing robust access control mechanisms combined with standard identity management solutions.

2.Engaging in trust negotiation to ensure secure interactions between users and systems.

3.Developing processing techniques for continuous queries to manage the dynamic nature of mobile data access.

# CONCLUSION:

Ensuring data security, especially safeguarding data against unauthorized access, stands as a pivotal objective within any data management system. This document encapsulates research discoveries, practical advancements, and deliberates on unresolved research queries. Additional areas pertinent to database security encompass inference control and statistical database security. Despite their investigation in prior years, these aspects maintain contemporary relevance, particularly within the sphere of privacy-preserving methodologies. Further significant matters not covered herein encompass security concerning GIS data—a domain gaining prominence in homeland security, including sensor data, information-grid designs, and privacy and security issues with Web services and the semantic Web. Because they are innovative, each of these applications has unique and untested security requirements that attract attention.

# REFERENCES:

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

[2]. 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.

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

[4]. 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.

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

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

[6]. What is database security: Threats & best practices: Imperva. Learning Center. (2022, October 26). https://www.imperva.com/learn/data-security/database-security/

[7]. Maurer, R. (2021, July 7). Top database security threats and how to mitigate them. SHRM. https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/top-database-security-threats.aspx

[8]. Challenges of database security. Online Tutorials, Courses, and eBooks Library. (n.d.). https://www.tutorialspoint.com/challenges-of-database-security.

[9]. Devane, H. (2023, April 5). The Complete Guide to Data Security Compliance laws and regulations. Immuta. https://www.immuta.com/blog/the-complete-guide-to-data-security-compliance-laws-and-regulations/.

[10]. Dr. Daniel Ivancevich. (n.d.). https://csbweb01.uncw.edu/people/ivancevichd/

[11]. 2 Examples of providers of such tools include Approva, www.approva.com; Aveksa, www.aveksa.com; and Security Compliance Corp., www.securitycompliancecorp.com.

[12]. Examples include Guardium, www.guardium.com; Imperva, www.imperva.com; or Tizor's Mantra, www.tizor.com.

[13]. 9 data security strategies you need to implement in 2023. PurpleSec. (2023, March 12). https://purplesec.us/learn/data-security-strategies/

[14]. Challenges of database security. Online Tutorials, Courses, and eBooks Library. (n.d.). https://www.tutorialspoint.com/challenges-of-database-security

[15]. A comprehensive approach to data security management. SurveyCTO. (2023, October 31). https://surveycto.com/resources/guides/data-security-guide/