MAC MODEL IN DBMS

NAME – ABHIRUP BAG
ROLL – 13000122082
DEPARTMENT – CSE(B)
SEMESTER – 6
PAPER – DATABASE MANAGEMENT SYSTEM (PCC-CS601)

CONTENT

INTRODUCTION

- **What is MAC?**
  - ✓ A security model where access to resources is strictly controlled by a central authority.
  - ✓ Uses security labels (e.g., confidential, secret, top secret) for users and data.
- **Purpose:**
  - ✓ Prevent unauthorized access to sensitive data.
  - ✓ Ensure compliance with security policies and regulations.

HOW DOES MAC WORK ?

Key Components :

- **Subjects:** Users or processes requesting access.
- **Objects:** Data or resources being accessed.
- **Security Labels:** Assigned to both subjects and objects (e.g., clearance levels).

Access Rules:

- Access is granted only if the user's clearance matches or exceeds the data's classification.
- **Example:** A user with "secret" clearance can access "secret" or "confidential" data but not "top secret."

KEY FEATURES OF MAC

- ✅ **Centralized Control –** Unlike parametric methods (e.g., normal distribution with mean and variance), non-parametric methods do not assume a predefined shape for the data distribution.
- ✅ **Security Labels –** These methods rely on the structure of the observed data to make inferences.
- ✅ **No Discretionary Access –** Non-parametric methods adapt to data patterns but often require larger sample sizes to achieve similar accuracy as parametric methods.
- ✅ **Data Classification –** Confidentiality is enforced.

MAC VS. DISCRETIONARY ACCESS CONTROL (DAC)

1 Mandatory Access Control

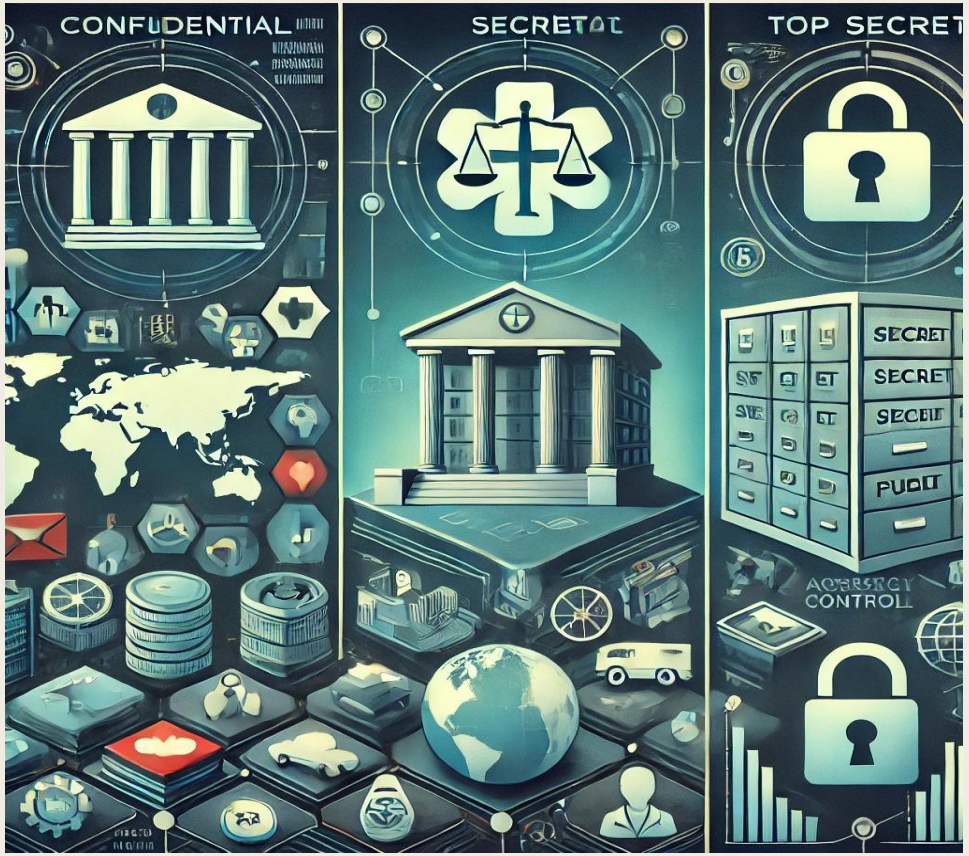
- Centrally managed by administrators.
- Strict, non-negotiable access rules.
- Ideal for high-security environments.

2 Discretionary Access Control

- Users can set permissions for their resources.
- More flexible but less secure.
- MAC enforces mandatory policies, while DAC allows discretionary control.

ADVANTAGES OF MAC IN DBMS

1. **Strong Security:** Prevents unauthorized access and data breaches.
2. **Consistent Enforcement:** Centralized control ensures uniform application of policies.
3. **Compliance:** Helps meet regulatory and legal requirements.
4. **Protection of Sensitive Data:** Ideal for classified or confidential information.



CHALLENGES OF MAC

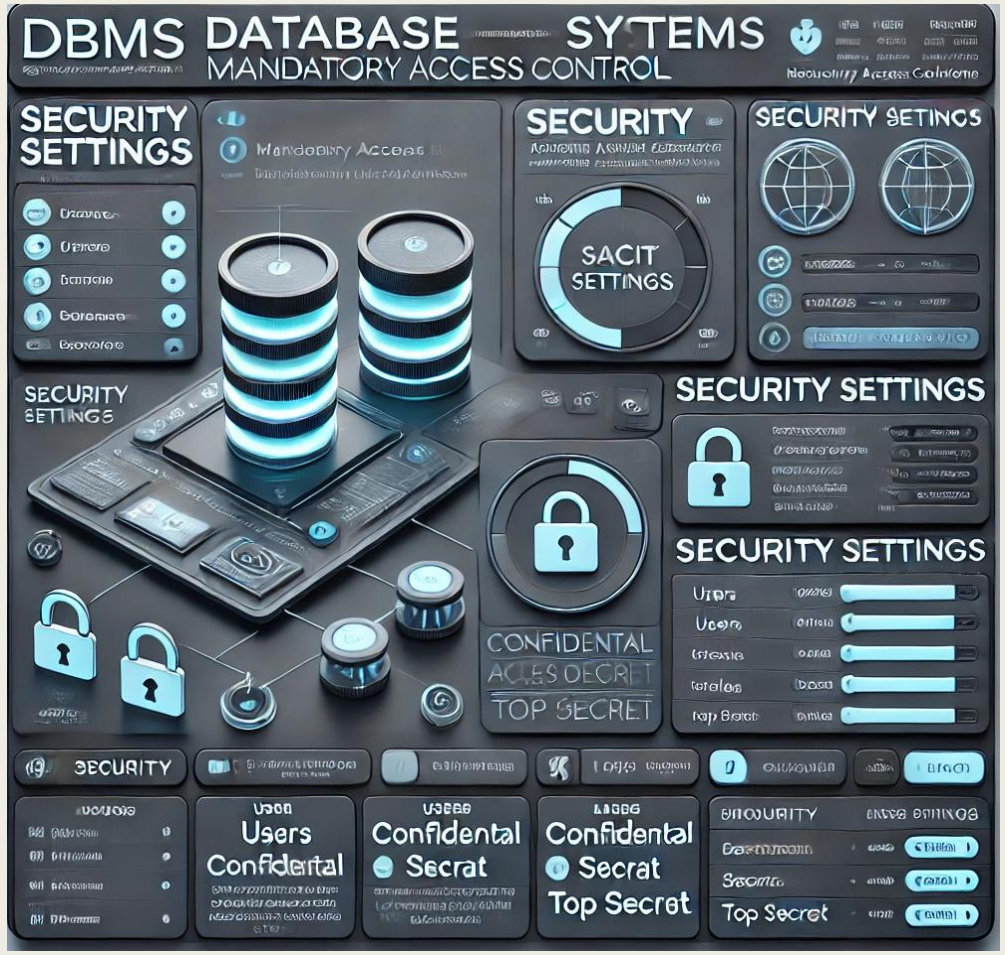
1. **Rigidity:** Strict policies can reduce flexibility and usability.
2. **Complexity:** Requires careful management of security labels and policies.
3. **Administrative Overhead:** Centralized control demands significant administrative effort.
4. **User Productivity:** Strict access rules may hinder workflow efficiency.

MAC IN DATABASE MANAGEMENT SYSTEMS (DBMS)

- **How MAC is Implemented in DBMS:**
  - Security labels are assigned to database objects (tables, rows, columns).
  - Users are granted access based on their clearance levels.

- **Example:**
  - A table containing employee salaries is labeled "confidential."
  - Only users with "confidential" or higher clearance can access it.

- **Benefits:**
  - Protects sensitive data in multi-user environments.
  - Ensures data integrity and confidentiality.



REAL-WORLD APPLICATIONS

- ✅ **Government Databases :–** Classified information storage and retrieval.
- ✅ **Healthcare Systems :–** Protects patient records and medical data.
- ✅ **Financial Institutions :–** Secures transactional and customer data.
- ✅ **Defense Systems :–** Manages access to mission-critical data.

CONCLUSION

- ✓ The Mandatory Access Control (MAC) Model is one of the most secure access control mechanisms used in high-security environments like military, government, and financial systems.
- ✓ It enforces strict access policies, ensuring confidentiality and integrity by preventing unauthorized access and data leaks.
- ✓ Though rigid and complex, MAC is essential for protecting classified information and is often used alongside DAC and RBAC for a balanced security approach.
- ✓ Understanding and implementing MAC enhances database security, making it a crucial model in DBMS security frameworks.

💡 "Security is not a product, but a process." – Bruce Schneier

REFERENCES

- **"Security Engineering: A Guide to Building Dependable Distributed Systems"** – *Ross J. Anderson*
- **"Computer Security: Art and Science"** – Matt Bishop
- **"Foundations of Security: What Every Programmer Needs to Know"** – Neil Daswani, Christoph Kern, and Anita Kesavan
- **"Access Control Systems: Security, Identity Management and Trust Models"** – Messaoud Benantar
- **"Introduction to Computer Security"** – Michael T. Goodrich and Roberto Tamassia

Thank you

ABHIRUP BAG

abhirup7477@gmail.com

ROLL NO. : 13000122082