Access control models define how systems manage and regulate access to resources. These models dictate who can access what, based on factors like user identity, roles, attributes, or predefined rules. Common models include Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Rule-Based Access Control (RUBAC), Attribute-Based Access Control (ABAC).

**Discretionary Access Control (DAC) :** DAC grants resource owners the flexibility to manage access permissions for their resources, allowing them to grant or revoke access to other users.

**Mandatory Access Control (MAC) :** MAC is a highly centralized and strict model where access is determined by security labels assigned to both subjects users and resources, controlled by a delegated administrator, ensuring users cannot override policies.

**Role-Based Access Control (RBAC) :** RBAC grants permissions based on user roles within an organization, simplifying access management in larger, well-defined organizational structures where roles are clear.

**Rule-based access control (RUBAC) :** A security mechanism that restricts access to resources based on predefined rules, often involving attributes of users, resources, and the environment. These rules are evaluated to determine if access should be granted or denied, providing a flexible way to enforce security policies.

**Attribute-Based Access Control (ABAC) :** ABAC provides a dynamic approach where access decisions are made based on a combination of attributes associated with the user, resource, and environment, following an "if-then-else" logic.