1. **Personal Identification:**

- **Description:** This method involves using unique credentials assigned to individuals, such as usernames, passwords, biometric data (fingerprints, facial recognition), or smart cards, to verify and grant access to specific resources or systems. It ensures that only authorized users can access sensitive information or perform certain tasks.

2. **Directory:**

- **Description:** A directory-based access control system organizes user accounts and permissions in a hierarchical structure, often managed through services like LDAP (Lightweight Directory Access Protocol). Users are granted access to resources based on their directory membership (e.g., groups, roles). This method allows for centralized management of access rights across an organization.

3. **File:**

- **Description:** File-level access control restricts access to specific files or directories. Permissions are set to determine which users or groups can read, write, or execute files. This method ensures that only authorized users can modify or view sensitive documents, protecting data integrity and confidentiality.

4. **Temporal:**

- **Description:** Temporal access control restricts access to resources based on time. Users may only access certain systems, networks, or data during specific hours or days. This method is often used to enhance security by limiting access to critical resources outside of business hours or during scheduled maintenance.