

Authorization

The difference between authorization and authentication is that authentication is when the system verifies your identity, while authorization decides what you are allowed to do once your identity is confirmed. For example, logging into your social media account is authentication, but whether you can view posts or manage the profile depends on authorization.

One common system is Role-Based Access Control (RBAC), where users are grouped into roles like “viewer,” “editor,” or “admin,” and each role has specific permissions. Another method is Access Control Lists (ACLs), which directly list what actions users can perform on certain files or resources.

A core practice is the Principle of Least Privilege (PoLP). This means users should only have the minimum access necessary to do their jobs. For example, a bank teller can handle deposits and withdrawals but should not be able to approve loans or modify account settings. This reduces the chance of mistakes or misuse and helps keep systems secure.