Authorization vs Authentication Computer security depends on two essential concepts which function independently from each other. The verification process of user identity and system or device identity makes up the authentication procedure. The system verifies that the requesting entity matches the identity information they provide during authentication. Users authenticate themselves through three main methods which include typing their username and password and supplying biometric information and using security tokens. The system uses authorization to establish what actions an authenticated user can perform. The system uses authorization to regulate resource access by allowing users to execute only their authorized actions. An employee who passes authentication checks will get access to read files but will not have permission to modify or remove them. Multiple approaches exist for implementing authorization systems. Role-Based Access Control (RBAC) provides a straightforward method to handle permissions through pre-defined roles such as admin and editor and viewer which makes permission management easier for multiple users. The Access Control List (ACL) system grants particular permissions to both users and groups for accessing specific resources. The principle of least privilege restricts user access to access only the essential permissions needed for their work activities to minimize security threats. The combination of authentication with authorization systems protects sensitive information while granting authorized users secure access to needed resources.