Authentication and Authorization:

Authentication and authorization are two critical security processes that work together to protect systems and data. While they are often confused as they sound similar, they serve distinct purposes:

Authentication:

- What it is: Authentication verifies the identity of a user or service attempting to access a system.
- How it works: Users provide credentials, such as usernames and passwords, or go through verification processes like biometric authentication. These credentials are compared to stored information to confirm their identity.
- Examples: Logging in to a website, providing your fingerprint to unlock your phone, or presenting your ID at an airport security checkpoint.

Authorization:

- What it is: Authorization determines what resources a user can access and what actions they can perform within a system.
- How it works: Once a user is authenticated, their access level is determined based on pre-defined rules and permissions. These rules dictate what data they can see, modify, or delete, and what actions they are authorized to perform.
- Examples: Only editors having permission to modify articles on a website, doctors having access to specific patient medical records, or security personnel having the ability to control access to restricted areas.