Activity 5.2 – Learning Highlights

Security And Privacy Of Application Systems Architectures:

- **Monolithic Architecture:** These are easier to build and get running, but scaling can be a nightmare. If one part of the app gets hacked, the whole thing is vulnerable.
- **Microservices Architecture:** It's like a house having many doors, maybe it's convenient for you but it's a good news for thieves too.
- **Client-Server Architecture:** You need secure channels to protect data transaction between the client and server.
- **Service-Oriented Architecture (SOA):** Complicated Structure, need to do more work to secure.
- **Web Application Architecture:** Since your app is living on the web, it's a huge target for hackers.
- **Cloud-Native Architecture:** In the cloud, security is a shared responsibility between you and the cloud provider. While they take care of the infrastructure, you need to handle things like managing user access, encrypting data, and ensuring you follow privacy laws and regulations.

Authentication V.S. Authorisation

Authentication verifies a user's identity, ensuring they are who they claim to be, often through passwords or biometrics. Authorization, on the other hand, determines what that user is allowed to do within the system. In simple words, authentication asks, "**Who are you?**" authorization asks, "**What can you access**?"

Techniques for Strong Authentication Mechanisms

- **Multi-factor Authentication (MFA):** Annoying, but your account will be more secured.
- **Strong Password Policies:** Use a mix of uppercase, lowercase, numbers and special characters as your password. At least 12 digits.
- **Account Lockout Policies:** For some financial related applications like bank app, it is necessary to implement this. It can prevent potential finance loss of the account owner.
- **Two-step Verification:** Add extra security layer to your account.