Assignment 2.11

1. What is cloud Architecture Design in terms of security ?

Cloud security architecture is a **security strategy designed around securing an organization's data and applications in the cloud**. It is a critical extension of enterprise security, and it requires an architecture to connect it with an overall security approach.

Cloud security is a collection of procedures and technology designed to address external and internal threats to business security. Organizations need cloud security as they move toward their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.

The terms digital transformation and cloud migration have been used regularly in enterprise settings over recent years. While both phrases can mean different things to different organizations, each is driven by a common denominator: the need for change.

Cloud security is a collection of procedures and technology designed to address external and internal threats to business security. Organizations need cloud security as they move toward their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.

The terms digital transformation and cloud migration have been used regularly in enterprise settings over recent years. While both phrases can mean different things to different organizations, each is driven by a common denominator: the need for change.

**Key elements of Cloud Security Architecture:-**

1. Security at Each Layer
2. Centralised Management of Components
3. Redundant & Resilient Design
4. Elasticity & Scalability
5. Appropriate storage for Deployments
6. Alerts & Notifications
7. Centralization , Standardization & Automation

## **Principles of Cloud Security Architecture**

**A well-designed cloud security architecture should be based on the following key principles:**

* Identification—Knowledge of the users, assets, business environment, policies, vulnerabilities and threats, and risk management strategies (business and supply chain) that exist within your cloud environment.
* Security Controls—Defines parameters and policies implemented across users, data, and infrastructure to help manage the overall security posture.
* Security by Design—Defines the control responsibilities, security configurations, and security baseline automations. Usually standardized and repeatable for deployment across common use cases, with security standards, and in audit requirements.
* Compliance—Integrates industry standards and regulatory components into the architecture and ensures standards and regulatory responsibilities are met.
* Perimeter Security—Protects and secures traffic in and out of organization’s cloud-based resources, including connection points between corporate network and public internet.
* Segmentation—Partitions the architecture into isolated component sections to prevent lateral movement in the case of a breach. Often includes principles of ‘least privilege’.
* User Identity and Access Management—Ensures understanding, visibility, and control into all users (people, devices, and systems) that access corporate assets. Enables enforcement of access, permissions, and protocols.
* Data encryption—Ensures data at rest and traveling between internal and external cloud connection points is encrypted to minimize breach impact.
* Automation—Facilitates rapid security and configuration provisioning and updates as well as quick threat detection.
* Logging and Monitoring—Captures activities and constant observation (often automated) of all activity on connected systems and cloud-based services to ensure compliance, visibility into operations, and awareness of threats.
* Visibility—Incorporates tools and processes to maintain visibility across an organization’s multiple cloud deployments.
* Flexible Design—Ensuring architecture design is sufficiently agile to develop and incorporate new components and solutions without sacrificing inherent security.

## **Cloud Security Architecture Threats**

Cloud services are affected by the most common types of concerns and threats including :

data breaches, malware injections, regulatory non-compliance, insider threats, advanced persistent threats (APTs), credential stuffing attacks, insecure application programming interfaces (APIs), zero-day attacks, account hijacking through stolen or compromised credentials, phishing, and service disruptions due to denial-of-service attacks or misconfigurations. If a breach occurs, liability for the breach is based on the shared responsibility model.

B) Choose a business domain e.g. Banking, Finance, Government Services, E-commerce, then succinctly explain how would you implement Cloud Architecture Design - Security on your system.

Business Domain: General E-Commerce Provider

### **1. Identify the state of cloud use and associated risks.**

**Step 1: Identify sensitive data.**

Correctly identify and tag your sensitive data to fully assess the risk.

**Step 2: Determine access to sensitive data.**

Identify, classify and map data locations, and flows. To do this, you must assess file and folder permissions in the cloud environment and access contexts, such as user roles, user location, and device type.

**Step 3: Verify cloud access from unknown sources.**

Determine what cloud services your organization’s members use and then assess their risk profile.

**Step 4: Check the configuration of cloud services.**

Audit the configuration of identity and access management, network configuration, and encryption.

**Step 5: Identify malicious use of data.**

Data monitoring for anomalies and limit internal and external data loss.

### **2. Protect the cloud environment.**

Protection should be implemented according to the associated risk levels.

**Step 1: Assign a protection rule.**

Control and protection rules must be assigned to determine which data can be stored in the cloud and which deserves better protection

**Step 2: Encrypt the data.**

To ensure data security when using cloud services, use the highest data encryption levels for transmission and storage. When encrypting sensitive data, it’s best to use your encryption keys so that you have complete control over who can access the data and are 100% confident in its security.

**Step 3: Establish rules for data sharing.**

Controlling which users can share/edit data and which should be restricted to viewers only.

**Step 4: Stop sharing data with unknown devices.**

Unmanaged devices should be blocked, requiring security verification (2FA) of the device before downloading.

**Step 5: Implement bot and malware protection.**

Malware protection technology can be applied to the operating system and virtual network to protect the infrastructure.

### **3. Respond to attacks and problems.**

Follow these best practices in responding to attack attempts and successful attacks.

**Step 1: Add authentication controls.**

Identify access scenarios that are identified as high-risk. In such cases, two-factor authentication to confirm your identity may be required.

**Step 2: Establish new policies for more cloud services.**

When new cloud services are integrated into existing infrastructure, access policies should be automatically updated to block access or display a warning message. This is achieved by integrating the cloud risk database with a secure network gateway or firewall.

**Step 3: Remove malware from the cloud service.**

To do this, scanning your cloud files with malware protection software is necessary to avoid ransomware attacks or data theft.

4) Incident Response: Putting in place the tools and access ahead of a security incident, then routinely practicing incident response through game days, will help to ensure that our architecture can accommodate timely investigation and recovery.