**Task 06**

**Data Privacy and Encryption**

This strategy outlines the data privacy practices and encryption methodologies adopted to protect sensitive information across its lifecycle—ensuring confidentiality, integrity, and compliance with global data protection standards.

**2. Data Privacy Implementation**

To uphold privacy by design and minimize the risk of unauthorized data exposure, a combination of anonymization techniques and privacy-aware processing models is employed.

**2.1. Anonymization Techniques**

* **Tokenization:**  
  Replaces sensitive identifiers (e.g., account numbers, Aadhaar IDs) with randomly generated tokens, detaching the data from its real-world identity while retaining utility for internal systems.
* **Pseudonymization:**  
  Personal identifiers are substituted with artificial identifiers (e.g., user123), allowing data usage without exposing actual identities. Original data is stored separately with strict access controls.

**Differential Privacy:**  
Statistical noise is added to analytical datasets to protect individual privacy while preserving overall data trends. Ideal for sharing insights without compromising individual records.

**Dynamic Data Masking:**  
Real-time masking of sensitive data (e.g., displaying only last 4 digits of a PAN) based on user roles and access levels, without altering the original stored values.

**3. Encryption Strategies**

Encryption is enforced at multiple levels to secure both **data at rest** and **data in transit**, as well as for **end-to-end transactions**.

**3.1. Data at Rest**

**AES-256 Encryption:**  
Industry-standard symmetric encryption used for database, file system, and backup encryption.

**Column-Level Encryption:**  
Sensitive fields (e.g., customer SSNs, financial data) are encrypted individually within databases for fine-grained protection.

**Full Disk Encryption (FDE):**Ensures that all contents of drives (especially portable or removable media) are encrypted and inaccessible without proper authentication.

**3.2. Data in Transit**

**TLS 1.3 Encryption:**Ensures all web and API communications are encrypted using the latest Transport Layer Security protocol, providing forward secrecy and minimizing latency.

**Secure VPN Access:**  
All remote or offsite access to the internal network is routed through secure VPN tunnels with strong encryption and MFA (Multi-Factor Authentication).

**3.3. End-to-End Encryption**

**Digital Banking Applications:**Full encryption from the user’s device to the backend servers ensures that sensitive information (login credentials, transaction data) is never exposed in plaintext at any point during transmission.

**4. Supporting Privacy Controls**

**Data Classification-Based Controls:**Encryption and privacy measures are enforced based on data classification (Public, Internal, Confidential, Highly Sensitive).

**Access Governance:**  
Integration with Role-Based Access Controls (RBAC) and audit trails to monitor and restrict who can view, decrypt, or process sensitive data.

**Key Management:**Centralized key management using Hardware Security Modules (HSMs) and periodic rotation of encryption keys per policy.