Data Privacy and Encryption

1. Anonymization Techniques

- **Tokenization of sensitive identifiers**: Replaces sensitive data with unique tokens for secure storage.
- **Pseudonymization of personal data**: Replaces real identities with pseudonyms to protect individuals.
- **Differential privacy for analytical purposes**: Adds noise to datasets to protect individual data points.
- **Dynamic data masking**: Hides sensitive data in real-time during query or view access.

2. Encryption Strategies

Data at Rest

- **AES-256 encryption**: Industry-standard symmetric encryption for maximum security.
- **Column-level encryption for sensitive fields**: Encrypts only critical data fields like SSN, card numbers.
- **Full disk encryption**: Secures entire storage drives against physical theft or unauthorized access.

Data in Transit

- **TLS 1.3 encryption**: Secures HTTP/HTTPS traffic with forward secrecy and reduced handshake latency.
- **Secure VPN for remote access**: Encrypts communications between remote employees and data centers.
- **End-to-end encryption for digital banking**: Protects messages and transactions from origin to destination.