

Q1. Key Classes, Attributes, and Functionalities

1. AutomatedFraudDetectionSystem (Central Controller)

Role: Acts as the main orchestrator of the system. It manages transaction processing, risk evaluation, decision making, and alert generation.

Key Attributes:

- systemId
- systemStatus (Active / Maintenance / Fail-safe)

Key Methods:

- processTransaction()
- calculateRiskScore()
- approveTransaction()
- blockTransaction()

2. User (Base Class)

Role: Abstract parent class representing all human users interacting with the system.

Key Attributes:

- userId
- username
- password (Encrypted)

Key Methods:

- login()
- logout()

3. BankCustomer (Inherits from User)

Role: Represents a bank customer who performs financial transactions and receives fraud alerts.

Key Attributes:

- accountNumber
- registeredDevices

Key Methods:

- initiateTransaction()
- receiveAlert()

4. SystemAdmin (Inherits from User)

Role: Responsible for system configuration, fraud rule management, and AI model control.

Key Attributes:

- adminId
- accessLevel

Key Methods:

- manageRiskRules()
- manageAIModels()
- generateComplianceAudit()

5. FraudAnalyst (Inherits from User)

Role: Handles manual investigation and review of suspicious transactions.

Key Attributes:

- analystId
- assignedCases

Key Methods:

- investigateTransaction()
- approveOverride()
- labelTransaction()

6. Transaction

Role: Represents a financial transaction submitted for fraud analysis.

Key Attributes:

- transactionId
- userId
- amount
- timestamp
- merchantId
- deviceId
- ipAddress

Key Methods:

- getTransactionDetails()
- validateTransaction()

7. TransactionMonitor

Role: Continuously monitors transaction flow and user behavior in real time.

Key Attributes:

- monitoringStatus
- transactionQueue

Key Methods:

- monitorTransaction()
- detectAnomaly()

8. RiskScoringEngine

Role: Calculates fraud risk score using rules, machine learning, and behavioral analysis.

Key Attributes:

- riskThresholdLow
- riskThresholdMedium
- riskThresholdHigh

Key Methods:

- computeRiskScore()
- classifyRiskLevel()

9. RuleEngine

Role: Applies predefined fraud detection rules and heuristics.

Key Attributes:

- ruleSet
- ruleVersion

Key Methods:

- evaluateRules()
- updateRules()

10. MLModelManager

Role: Manages machine learning models for adaptive fraud detection.

Key Attributes:

- modelVersion
- trainingDataSet

Key Methods:

- predictFraudProbability()
- retrainModel()

11. AlertManager

Role: Sends real-time alerts and notifications to users and administrators.

Key Attributes:

- alertChannel (SMS / Email / Push)

Key Methods:

- sendRealTimeAlert()
- notifyCustomer()

12. ExternalFraudDatabase

Role: Integrates external fraud intelligence sources for enhanced detection.

Key Attributes:

- apiEndpoint
- apiKey

Key Methods:

- queryFraudPatterns()
- fetchBlacklistData()

13. DashboardAndReports

Role: Displays fraud analytics, statistics, and compliance reports.

Key Attributes:

- fraudMetrics
- reportData

Key Methods:

- displayDashboard()
- generateReport()