AI/ML Use Cases with Actors and Technologies

1. Passenger Experience Use Cases

1.1 Personalized Navigation and Gate Change Alerts

Actors:
- Passenger
- Airport Information Systems
- Airline Systems

Technological Medium:
- Mobile Application
- WiFi Network
- iBeacon Infrastructure
- Airport Kiosks

Scenario Flow:
1. Passenger performs self-service check-in via kiosk
2. Passenger connects to airport WiFi via mobile app
3. Passenger approaches gate unaware of gate change
4. WiFi/iBeacon detects passenger location
5. App alerts passenger of gate change
6. App provides floor map with turn-by-turn navigation

AI/ML Components:
- **Location Tracking**: Real-time passenger positioning using WiFi triangulation and iBeacon proximity detection
- **Path Optimization**: Calculates fastest route to new gate based on current location, walking speed, and crowd density
- **Time Estimation**: Predicts walking time to gate considering historical movement patterns and current airport conditions

Implementation Partners:
- Thales: iBeacon infrastructure and location services
- Salesforce: Passenger data management and notifications
- Equinix: Real-time data processing infrastructure

1.2 Personalized Retail Recommendations

Actors:
- Passenger
- Retail Partners
- Marketing Systems

Technological Medium:
- Mobile Application
- iBeacon Infrastructure
- CRM System

Scenario Flow:
1. Passenger navigates through airport to gate
2. App detects passenger is passing near duty-free areas
3. AI analyzes passenger purchase history and profile
4. App presents personalized duty-free offers en route to gate

AI/ML Components:
- **Recommendation Engine**: Analyzes passenger purchase history, demographics, and preferences
- **Contextual Awareness**: Considers flight time, available shopping time, and passenger location
- **Conversion Prediction**: Calculates likelihood of purchase for different product categories
- **Offer Optimization**: Determines optimal timing and content of offers to maximize conversion

Implementation Partners:
- Salesforce: CRM and personalization engine
- Thales: iBeacon infrastructure
- Equinix: Data processing and analytics

2. Airport Staff Security Use Cases

2.1 Threat Detection and Response

Actors:
- Airport Security Staff
- Passengers
- Backup Security Team
- Borderplex Command Center

Technological Medium:
- Handheld Devices
- CCTV System with Facial Recognition
- APIS (Advance Passenger Information System)
- Interpol Database
- Risk Assessment System

Scenario Flow:
1. System detects probable match between APIS and Interpol watchlist during check-in
2. AI performs real-time risk assessment based on multiple factors
3. Airport staff receives alert via handheld app
4. Backup security team is placed on standby
5. Borderplex command center is alerted of potential threat
6. Passenger is tracked via CCTV facial recognition
7. Staff uses app for navigation to passenger's location
8. Staff verifies passenger using multimodal biometrics
9. Threat is de-escalated and data captured for future analysis

AI/ML Components:
- **Facial Recognition**: Matches passenger faces against watchlist databases with confidence scoring
- **Multi-factor Risk Assessment**: Evaluates threat level using passenger data, travel patterns, and behavioral indicators
- **Real-time Tracking**: Maintains continuous subject identification across multiple CCTV cameras
- **Staff Routing**: Calculates optimal paths for security personnel to intercept subjects
- **Biometric Verification**: Performs multi-modal biometric matching (face, fingerprint) with liveness detection
- **Threat Pattern Learning**: Improves detection algorithms through feedback from resolved cases

Implementation Partners:
- Thales: Biometric verification and handheld devices
- RapidScan: Supplementary scanning data
- Equinix: Secure infrastructure for sensitive data processing
- Salesforce: Case management and resolution tracking

3. Pilot and Crew Use Cases

3.1 Digital Checklist and Exception Management

Actors:
- Pilots
- Cabin Crew
- Ground Staff
- Air Traffic Control

Technological Medium:
- Electronic Flight Bag (Tablet/Handheld)
- Aircraft Systems Interface
- Operations Control Center

Scenario Flow:
1. Pilot accesses digital checklist on electronic flight bag
2. System guides through normal checklist procedures
3. AI monitors completion status and flags potential issues
4. System handles exceptions and special approvals when needed

AI/ML Components:
- **Checklist Optimization**: Adapts checklist sequence based on aircraft state and conditions
- **Anomaly Detection**: Identifies unusual readings or procedure deviations
- **Decision Support**: Provides recommendations for handling non-standard situations
- **Predictive Maintenance**: Flags potential mechanical issues based on system readings
- **Workflow Automation**: Manages approvals and escalations for exceptions

Implementation Partners:
- Thales: Electronic flight bag and aircraft interfaces
- Salesforce: Workflow management and approvals
- Equinix: Real-time data processing

3.2 Operational Efficiency and Safety

Actors:
- Pilots
- Cabin Crew
- Operations Control
- Maintenance Teams

Technological Medium:
- Electronic Flight Bag
- Aircraft Systems
- Operations Dashboard

Scenario Flow:
1. System monitors flight operations in real-time
2. AI identifies potential efficiency improvements or safety concerns
3. Recommendations are provided to crew via electronic flight bag
4. System learns from crew actions and outcomes

AI/ML Components:
- **Fuel Optimization**: Recommends optimal settings based on flight conditions and historical data
- **Safety Pattern Recognition**: Identifies potential safety issues before they become critical
- **Procedure Compliance**: Monitors adherence to standard operating procedures
- **Crew Resource Management**: Suggests optimal task distribution based on workload analysis
- **Continuous Learning**: Improves recommendations based on outcomes and crew feedback

Implementation Partners:
- Thales: Cockpit systems and interfaces
- Equinix: Data processing and analytics
- Salesforce: Reporting and feedback management

4. Land Border Staff Use Cases

4.1 Multi-Modal Threat Detection

Actors:
- Border Control Officers
- Vehicle Passengers
- Backup Security Team
- Borderplex Command Center

Technological Medium:
- Vehicle Scanning Systems
- Handheld Biometric Devices
- CCTV Systems
- Criminal Databases

Scenario Flow:
1. Passenger vehicle approaches land border checkpoint
2. Scanner detects suspicious item in cargo
3. Facial recognition identifies probable match with criminal database
4. AI performs comprehensive risk assessment
5. Border staff receives alert via handheld with instructions
6. Staff conducts additional checks following SOP
7. System alerts backup team and command center if threat escalates

AI/ML Components:
- **Object Detection**: Identifies suspicious items in vehicle scans using computer vision
- **Facial Recognition**: Matches vehicle occupants against watchlist databases
- **Risk Scoring**: Calculates threat level based on multiple inputs (scan results, identity matches, behavior)
- **Pattern Recognition**: Detects unusual concealment methods based on historical data
- **Anomaly Detection**: Identifies vehicles or persons deviating from normal patterns
- **Coordinated Threat Analysis**: Correlates incidents across multiple border points to detect organized activities

Implementation Partners:
- RapidScan: Vehicle and cargo scanning technology
- Thales: Biometric verification and handheld devices
- Equinix: Data processing infrastructure
- Salesforce: Case management and reporting

4.2 Historical and Geographical Pattern Analysis

Actors:
- Border Intelligence Analysts
- Border Control Officers
- Security Agencies

Technological Medium:
- Intelligence Dashboard
- Geospatial Mapping System
- Historical Database
- Predictive Analytics Platform

Scenario Flow:
1. System continuously analyzes border crossing data
2. AI identifies patterns in crossing times, routes, and individuals
3. System correlates with external intelligence and historical incidents

4. Alerts are generated for potential coordinated threats
5. Intelligence is shared with relevant border posts

AI/ML Components:
- **Temporal Analysis**: Identifies unusual timing patterns in border crossings
- **Geospatial Clustering**: Detects unusual concentration of activities at specific locations
- **Network Analysis**: Maps relationships between individuals and vehicles crossing borders
- **Predictive Modeling**: Forecasts potential threat activities based on historical patterns
- **Anomaly Detection**: Identifies deviations from established patterns that may indicate threats

Implementation Partners:
- Equinix: Data processing and analytics infrastructure
- Salesforce: Intelligence dashboard and reporting
- Thales: Secure communication systems

Technology Integration Matrix

Use Case	iBeacon	Mobile App	Biometric Devices	CCTV	Scanning Systems	AI/ML Platform	CRM
Passenger Navigation	✓	✓				✓	✓
Retail Recommendations	✓	✓				✓	✓
Threat Detection		✓	✓	✓		✓	✓
Pilot Checklists		✓				✓	✓
Land Border Security		✓	✓	✓	✓	✓	✓

AI/ML Capability Requirements

Capability	Description	Primary Use Cases	Technology Partners
Facial Recognition		Security, Border Control	Thales

Capability	Description	Primary Use Cases	Technology Partners
	Biometric matching against databases with confidence scoring		
Object Detection	Identification of suspicious items in scans	Border Control	RapidScan
Recommendation Engine	Personalized offers based on passenger profiles	Passenger Experience	Salesforce
Location Intelligence	Real-time positioning and navigation	Passenger Experience, Security	Thales
Risk Assessment	Multi-factor threat evaluation	Security, Border Control	Equinix, Salesforce
Pattern Recognition	Detection of unusual behaviors or trends	Security, Border Control	Equinix
Predictive Analytics	Forecasting based on historical data	All Use Cases	Equinix, Salesforce

Implementation Roadmap

Phase 1: Foundation (Q3-Q4 2025)

- Data collection infrastructure setup
- Baseline AI models development
- Core passenger experience features

Phase 2: Core Security (Q1-Q3 2026)

- Biometric matching systems
- Basic threat detection
- Initial staff alerting capabilities

Phase 3: Advanced Features (Q3 2026-Q1 2027)

- Multi-modal threat detection

- Pattern analysis capabilities
- Enhanced recommendation engines

Phase 4: Intelligence Integration (Q2-Q4 2027)

- Cross-border intelligence sharing
- Predictive threat modeling
- Self-improving AI systems