# Inputs Documentation: AI-Powered Banking Assistant

## Project Overview

\*\*Project Name:\*\* AI-Powered Banking Support Assistant with Fraud Detection

\*\*AI Name:\*\* Vizhibot

\*\*Core Functionality:\*\* Customer support chatbot + Real-time fraud detection system

## Data Input Categories

### 1. User Authentication Inputs

| Input Field | Data Type | Source | Required | Example | Purpose |

|-------------|-----------|---------|----------|---------|---------|

| User ID | String | Login System | Yes | "cust\_12345" | User identification |

| Session Token | String | Auth System | Yes | "tok\_abc123xyz" | Session management |

| Device ID | String | User Device | No | "dev\_67890" | Device recognition |

| IP Address | String | Network | No | "192.168.1.100" | Location tracking |

### 2. Chatbot Inputs (Vizhibot QA System)

#### A) User Query Inputs

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Raw Message | String | User Input | "What's my account balance?" | Primary query |

| Message Timestamp | DateTime | System | "2025-08-30 14:30:45" | Conversation tracking |

| Message Language | String | Detection | "en" | Language processing |

| Conversation Context | JSON | Session | Previous messages | Context awareness |

#### B) Knowledge Base Inputs

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Banking Policies | Text | Database | Interest rates, fees | Policy information |

| FAQ Database | Text | CMS | Common questions | Quick answers |

| Product Information | Text | Product DB | Loan details | Product knowledge |

| Compliance Rules | Text | Legal | Regulatory info | Compliance answers |

### 3. Fraud Detection Inputs

#### A) Transaction Data Inputs

| Input Field | Data Type | Source | Example | Importance |

|-------------|-----------|---------|---------|------------|

| Transaction Amount | Float | Payment Gateway | 15000.50 (₹) | Primary risk indicator |

| Transaction Time | DateTime | System | "2025-08-30 03:15:30" | Time pattern analysis |

| Merchant Name | String | Payment Gateway | "Premium Electronics" | Merchant risk scoring |

| Merchant Category | String | MCC Code | "Electronics" | Category risk analysis |

| Merchant Location | String | Payment Gateway | "Mumbai, IN" | Geographic analysis |

| Payment Method | String | User Input | "Credit Card" | Payment type risk |

| Currency Type | String | Payment Gateway | "INR" | Currency risk |

| Transaction Channel | String | System | "Mobile App" | Channel risk analysis |

#### B) User Behavioral Inputs

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Spending Patterns | JSON | User History | Weekly averages | Behavior baseline |

| Typical Hours | Array | User History | [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20] | Time pattern analysis |

| Common Categories | Array | User History | ["Groceries", "Restaurants"] | Category preferences |

| Average Transaction | Float | User History | 2500.00 (₹) | Amount pattern |

| Spending Frequency | Integer | User History | 15 transactions/week | Frequency analysis |

#### C) Environmental Inputs

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Device Type | String | User Agent | "Android Mobile" | Device risk scoring |

| Browser Info | String | User Agent | "Chrome 115" | Browser fingerprinting |

| GPS Location | String | Device | "12.9716° N, 77.5946° E" | Location verification |

| Network Type | String | Device | "WiFi" | Network security |

| IP Geolocation | String | IP API | "Bangalore, India" | Location consistency |

#### D) Historical Data Inputs

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Past Transactions | JSON | Transaction DB | Last 6 months data | Historical pattern analysis |

| Previous Fraud Flags | Integer | Fraud DB | 2 incidents | Risk history |

| Chargeback History | Integer | Payment DB | 1 chargeback | Dispute history |

| Login History | JSON | Auth DB | Login patterns | Access pattern analysis |

### 4. External Data Inputs

#### A) Third-Party Data Sources

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Blacklisted Merchants | JSON | Security Feed | Known fraudulent merchants | Merchant risk scoring |

| IP Threat Intelligence | JSON | Threat Intel | Malicious IP addresses | IP risk scoring |

| Device Reputation | JSON | Security API | Compromised devices | Device risk scoring |

| Geographic Risk Data | JSON | GeoIP Service | High-risk regions | Location risk scoring |

#### B) Real-Time Market Data

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Currency Exchange Rates | JSON | Financial API | USD/INR rates | Cross-border transaction risk |

| Market Trends | JSON | Market Data | Spending trends | Anomaly detection |

| Holiday Calendar | JSON | Calendar API | Festival dates | Seasonal pattern analysis |

### 5. System Configuration Inputs

#### A) Model Configuration

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Risk Thresholds | JSON | Config File | {"high\_risk": 0.7} | Decision boundaries |

| Model Parameters | JSON | ML Config | RandomForest parameters | Model behavior |

| Feature Weights | JSON | Config File | {"amount\_weight": 0.6} | Feature importance |

#### B) Business Rules

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Compliance Rules | JSON | Legal Team | RBI guidelines | Regulatory compliance |

| Business Policies | JSON | Business | Max transaction limits | Business rules |

| Alert Triggers | JSON | Security | Alert conditions | Notification rules |

### 6. Output & Feedback Inputs

#### A) User Feedback

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Response Rating | Integer | User Input | 5 (stars) | Chatbot improvement |

| False Positive Flag | Boolean | User Input | true | Model retraining |

| Feature Request | String | User Input | "Add budgeting feature" | System enhancement |

#### B) System Monitoring

| Input Field | Data Type | Source | Example | Purpose |

|-------------|-----------|---------|---------|---------|

| Performance Metrics | JSON | Monitoring | Accuracy scores | System health |

| Error Logs | JSON | Logging System | Error messages | Debugging |

| Usage Statistics | JSON | Analytics | Feature usage | Product improvement |

## Data Flow Diagram

A computer screen shot of a diagram

AI-generated content may be incorrect.

## Security Considerations

1. \*\*PII Handling\*\*: All personal data encrypted at rest and in transit

2. \*\*Data Retention\*\*: Transaction data stored for 7 years for compliance

3. \*\*Access Control\*\*: Role-based access to sensitive data

4. \*\*Audit Logging\*\*: All inputs logged for security auditing

## Compliance Requirements

- RBI Guidelines for Digital Banking

- GDPR Data Protection Standards

- PCI DSS for Payment Processing

- Local Banking Regulations

## Future Input Considerations

1. \*\*Biometric Data\*\*: Fingerprint/Facial recognition for authentication

2. \*\*Voice Inputs\*\*: Voice-based banking commands

3. \*\*Social Media Data\*\*: For enhanced customer profiling (with consent)

4. \*\*IoT Device Data\*\*: Smart device spending patterns

5. \*\*Blockchain Data\*\*: Cryptocurrency transaction monitoring

---

\*Last Updated: August 30, 2025\*

\*Document Version: 2.0\*