ATM Monitoring System - API Design

# **Introduction**

This document provides the API design for the ATM Monitoring System, which securely monitors the status and behaviour of ATMs within a bank’s network in real time. The API exposes endpoints to manage authentication, retrieve customer transaction data, monitor failures, and allow access to camera footage.

# **API Design Overview**

The API is RESTful and uses standard HTTP methods (GET, POST, PUT, DELETE) to expose data. The primary resources available in the API include: ATM status, transaction records, failure logs, and camera footage. Authorization is handled using JWT tokens, and secure communication is ensured with HTTPS.

# **1. Authentication Endpoints**

These endpoints are responsible for authenticating users and generating access tokens (JWT) for secure communication.

## **1.1 POST /api/v0.1/tokens/user**

Description: Get an admin token for services

Request Body:

{  
 "username": "admin",  
 "password": "password123"  
 }

Response Body:

{

"token": "eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJzZWxmIiwi.."

}

**1.2 POST /api/v0.1/tokens/machine**

**.addHeader("Authorization", "Bearer eyJhbGciOiJSUzI1NiJ9…”)**

Description: Get device token for an ATM

Request:

{ "bank": "icici", "deviceId": "10001", "expiry": 24 }

Response:

{

"token": "eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJzZWxmIiwi.."

}

# **2. Transaction Endpoints**

These endpoints are used to retrieve transaction-related data, such as the total number of customers and the breakdown of transactions.

## **2.1 GET /api/v0.1/atm/banks/last24hours**

Fetches the total number of customers who made transactions in the last 24 hours.

Response Body:  
 {  
 "totalCustomers": 150,  
 }

## **2.2 GET /api/v0.1/atm/banks/transaction-breakdown**

Fetches a breakdown of transactions by type (Deposit, Cash Withdrawal, Balance Information).

Response Body:

{  
 "deposit": 50,  
 "withdrawal": 40,  
 "balance\_info": 60  
 }

# **3. Failure Monitoring Endpoints**

These endpoints provide information about failures in the ATM network, such as system downtime or device errors.

## **3.1 GET /api/v0.1/atm/banks/failures**

Fetches a list of failures that occurred in the last 24 hours.

Response Body:

[

{

"id": 1,

"bank": "DemoBank",

"deviceId": "B223",

"transactionType": "WITHDRAW",

"failureType": "DOWN\_TIME",

"stamp": "2024-11-28T16:04:13.209+00:00",

"customerId": "cust-1121"

},

]

**4. Authorization and Security**

All API endpoints are secured using JWT tokens. The API requires an access token in the Authorization header of each request.

## **4.1 Authorization Header**

To access the API endpoints, users must include the JWT token in the Authorization header.

Example:

Authorization: Bearer <jwt\_token>

**4. Video Download**

These endpoints provide a list of files for a particular time range.

## **3.1 GET /api/v0.1/atm/banks/download-video/{fromtime}/{totime}**

Fetches a list of files for given time ranges.

Response Body:

[

{

"id": 3,

"stamp": "2024-11-28T23:19:10.029+00:00",

"deviceId": "B223",

"path": " <https://consappsrvr.irevo.in/images/store_setup/growVideo.mp4>"

},

{

"id": 4,

"stamp": "2024-11-28T23:19:40.007+00:00",

"deviceId": "B223",

"path": " <https://consappsrvr.irevo.in/images/store_setup/growVideo.mp4>"

},

]

# **Conclusion**

This API design document provides an overview of the endpoints that are essential for monitoring ATM devices, handling transaction data, tracking failures, and retrieving camera footage. The API is built to be secure, scalable, and able to integrate with existing bank systems.